DRN-5627291

The complaint

Mr U complains Revolut Ltd ("Revolut") didn't do enough to protect him when he fell victim to a scam.

What happened

Mr U said he had been interested in trading in cryptocurrency and had used a cryptocurrency provider, I'll refer to as B, to do so.

Mr U told us the scammer contacted him via a messaging app claiming to have got his details from B and offered a 30-day workshop experience whereby he could invest as part of a group to receive better returns. Mr U said he was added to a group chat with others taking part in the opportunity which made it seem genuine. Mr U said he invested on the scammer's instruction, and they seemed professional and knowledgeable. Mr U said he made payments to a cryptocurrency provider, I'll refer to as C, and was supposedly making good profits.

Mr U said when the 30-day period ended he was told before he could withdraw his funds, he needed to pay fees and taxes which he paid. The scammer requested further fees and Mr U said it was at this point he realised he'd been scammed.

These are the payments Mr U has complained about. He made them from his account via a legitimate cryptocurrency exchange and then on to scammers:

Payment	Date	Type of transaction	Payee	Amount
1	23 May 2023	Transfer	C	£100
2	23 May 2023	Transfer	C	£500
3	25 May 2023	Transfer	C	£400
4	29 May 2023	Transfer	C	£500
5	30 May 2023	Transfer	C	£1,000
6	1 June 2023	Transfer	C	£1,000
7	2 June 2023	Transfer	C	£5,000
8	3 June 2023	Transfer	C	£2,000
9	5 June 2023	Transfer	C	£2,000
10	5 June 2023	Transfer	C	£4,000
11	6 June 2023	Transfer	C	£2,500
12	18 June 2023	Transfer	C	£10,000
13	18 June 2023	Transfer	C	£65
14	30 June 2023	Transfer	C	£8,200
15	26 August 2023	Transfer	C	£190
16	27 August 2023	Transfer	C	£20
17	28 August 2023	Transfer	C	£450

Mr U complained to Revolut and unhappy with its response, he raised the matter with the Financial Ombudsman. One of our Investigators looked into the complaint and upheld it. They thought Revolut ought to have been concerned by payment 7 and provided a proportionate warning. They were persuaded if it had it would have prevented Mr U from

making the payment and those that followed. They felt Mr U should receive a full refund for payments 7 to 11 and that it was fair for Mr U and Revolut to share liability equally for payment 12 and those that followed.

Revolut didn't agree. In summary, it said:

- The payments were made from Mr U's Revolut account to an account in his own name and so are self to self payments, meaning the fraudulent transactions didn't originate from Mr U's Revolut account.
- As an Electronic Money Institution rather than a bank its accounts are typically set up to facilitate payments for a specific purpose rather than a main account and so the transactions weren't unexpected or unusual for how its customers use their accounts.
- It is an intermediary in the chain of the scam as the source of the funds lost to this scam originated from a firm other than Revolut. It said the Financial Ombudsman should consider the actions of other firms in the chain.

Mr U also didn't agree with the outcome, he said:

- If Revolut had intervened on payment 7 as the Investigator suggested, he wouldn't have made further payments to the scam and so he should receive a full refund from this point rather than 50% of some of the payments.

As an agreement could not be reached, the complaint has been passed to me for a final decision.

My provisional decision

I issued my provisional decision on 3 June 2025. I decided, provisionally, that I was going to uphold Mr U's complaint in part. This is what 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.

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.

And, as the Supreme Court has recently reiterated in Philipp v Barclays Bank UK PLC, subject to some limited exceptions banks have a contractual duty to make payments in compliance with the customer's instructions.

In that case, the Supreme Court considered the nature and extent of the contractual duties owed by banks to their customers when making payments. Among other things, it said, in summary:

- The starting position is that it is an implied term of any current account contract that, where a customer has authorised and instructed a bank to make a payment, it must

carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risk of its customer's payment decisions.

- At paragraph 114 of the judgment the court noted that express terms of the current account contract may modify or alter that position. In Philipp, the contract permitted Barclays not to follow its consumer's instructions where it reasonably believed the payment instruction was the result of APP fraud; but the court said having the right to decline to carry out an instruction was not the same as being under a legal duty to do so.

In this case, the terms of Revolut's contract with Mr U modified the starting position described in Philipp, by expressly requiring Revolut to refuse or delay a payment "if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks".

So Revolut was required by the implied terms of its contract with Mr U and the Payment Services Regulations to carry out their instructions promptly, except in the circumstances set out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

Whether or not Revolut was required to refuse or delay a payment for one of the reasons set out in its contract, the basic implied requirement to carry out an instruction promptly did not in any event mean Revolut was required to carry out the payments immediately[1]. Revolut could comply with the requirement to carry out payments promptly while still giving fraud warnings, or making further enquiries, prior to making the payment.

And, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Revolut should in June 2023 fairly and reasonably have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances (irrespective of whether it was also required by the express terms of its contract to do so).

In reaching the view that Revolut should have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances, I am mindful that in practice all banks and EMI's like Revolut do in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;[2]
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system for authorised push payments;
- providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified.

In reaching my conclusions about what Revolut ought fairly and reasonably to have done, I am also mindful that:

---

[1] The Payment Services Regulation 2017 Reg. 86 states that "the payer's payment service provider must ensure that the amount of the payment transaction is credited to the payee's payment service provider's account **by the end of the business day following the time of receipt of the payment** order" (emphasis added).

[2] For example, Revolut's website explains it launched an automated anti-fraud system in August 2018:
https://www.revolut.com/news/revolut_unveils_new_fleet_of_machine_learning_technology_that_has_seen_a_fourfold_reduction_in_card_fraud_and_had_offers_from_banks_/

- Electronic Money Institutions like Revolut are required to conduct their business with "due skill, care and diligence" (FCA Principle for Businesses 2), "integrity" (FCA Principle for Businesses 1) and a firm "must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems" (FCA Principle for Businesses 3)[3].

- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the "Financial crime: a guide for firms".

- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.

- The October 2017, BSI Code[4], which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).

- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

Overall, 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;

---

[3] Since 31 July 2023 under the FCA's new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.
[4] BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

- 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 – (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 U was at risk of financial harm from fraud?

It isn't in dispute that Mr U has fallen victim to a cruel scam here, nor that he authorised the payments to purchase cryptocurrency which were subsequently transferred to the scammer. Whilst I have set out in this decision the circumstances which led Mr U to make the payments using his Revolut account and the process by which that money ultimately fell into the hands of the scammer, 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 U might be the victim of a scam.

By June 2023, when these transactions took place, 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.

By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions[5]. And by June 2023, when these payments took place, further restrictions were in place[6]. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

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 (as Revolut has told our service). However, our service has also seen numerous examples of consumers being directed by fraudsters to use Revolut accounts in

[5] See for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022. NatWest Group, Barclays, Lloyds Banking Group and Santander had all introduced some restrictions on specific cryptocurrency exchanges by August 2021.
[6] In March 2023, Both Nationwide and HSBC introduced similar restrictions to those introduced by Santander in November 2022.

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 U made in June 2023, 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.

To be clear, I'm not suggesting as Revolut argues that, as a general principle, Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees. As I've set out in some detail above, it is the specific risk associated with cryptocurrency in June 2023 that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm.

In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. And as I have explained Revolut was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks.

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 U's own name should have led Revolut to believe there wasn't a risk of fraud.

So 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 U might be at a heightened risk of fraud that merited its intervention.

Based on what Revolut knew about payments 1 to 6 I don't think it ought to have been concerned that Mr U was potentially at risk of financial harm from fraud. I say this due to the low value of these payments and while they were going to a known cryptocurrency provider, 'crypto' was a reason Mr U gave when opening his account. I therefore don't think Revolut was unreasonable in processing these payments in line with Mr U's payment instructions.

I believe the value of payment 7 ought to have merited an intervention from Revolut as it was significantly higher than the previous payments Mr U made to C. The value coupled with the destination being identifiably cryptocurrency, I think should have been suspicious to Revolut and merited an intervention prior to processing the payment.

To be clear, I do not suggest that Revolut should provide a warning for every payment made to cryptocurrency. Instead, as I've explained, I think it was a combination of the characteristics of this payment (combined with those which came before it, and the fact the payment went to a cryptocurrency provider) which ought to have prompted an intervention from Revolut.

Revolut argues that it is unlike high street banks in that it provides cryptocurrency services in addition to its electronic money services. It says that asking it to 'throttle' or apply significant friction to cryptocurrency transactions made through third-party cryptocurrency platforms might amount to anti-competitive behaviour by restricting the choice of its customers to use competitors. As I have explained, I do not suggest that Revolut should apply significant friction to every payment its customers make to cryptocurrency providers. However, for the

reasons I've set out above I'm satisfied that by June 2023 Revolut should have recognised at a general level that its customers could be at increased risk of fraud when using its services to purchase cryptocurrency and, therefore, it should have taken appropriate measures to counter that risk to help protect its customers from financial harm from fraud. Such proportionate measures would not ultimately prevent consumers from making payments for legitimate purposes.

What did Revolut do to warn Mr U?

Revolut has confirmed it didn't intervene on any of the payments.

Revolut said Mr U was presented with a 'Transfer Review Warning' when he first added the new beneficiary as this is shown each time a transfer payment is made to a new beneficiary from an account for the first time. This warning asks if a customer knows and trusts the payee and if they're not sure, not to pay them. It goes on to say fraudsters can impersonate others.

Revolut told us it blocked Mr U's account on 18 June 2023 after its security system was triggered due to Mr U being a potential APP victim, and while it was blocked no payments or transfers could be completed. I've seen Revolut sent Mr U an email regarding the account restriction and directed him to get in touch via Revolut's in-app chat, which Mr U did on 20 June 2023. I've summarised the conversation below.

Revolut told Mr U it thought the transactions were highly likely to be scam related. After verifying himself he was asked if he's downloaded remote access software, if he was advised to open an account with Revolut after learning about an investment opportunity on social media, if he's recently received any unsolicited calls or messages about a safe account or if he was buying cryptocurrency. Mr U answered 'no' to all four questions. He was then asked if he recognised specific transactions and he confirmed he did after which he was asked if he was purchasing cryptocurrency and he said he was building a 'kitty to eventually buy crypto'.

Revolut goes on to highlight that cryptocurrency should only be purchased from a reputable company, and asks which exchange Mr U is using, does he have access to the account, if he's been able to withdraw, how he decided which exchange to use, where he learnt about it and how long he's been investing in cryptocurrency. Mr U confirms he uses B and C and he's been investing for a number of years. Revolut advises of being pressured to invest and repeats some of the previous scam education and he's asked to confirm he's been warned of the scam risks and recovery of funds is unlikely should it turn out he's been the victim of a scam.

What kind of warning should Revolut have provided?

I've thought carefully about what a proportionate warning for payment 7, 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.

Taking that into account, I think Revolut ought, when Mr U attempted to make payment 7, knowing that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency scams, without significantly losing impact.

So, at this point in time, I think that such a warning should have addressed the key risks and features of the most common cryptocurrency scams – cryptocurrency investment scams. 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, an 'account manager', 'broker' or 'trader' acting on their behalf; and a small initial deposit which quickly increases in value.

I recognise that a warning of that kind could not have covered off all scenarios. But I think it would have been a proportionate way for Revolut to minimise the risk of financial harm to Mr U by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr U suffered from payment 7?

I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case. And on balance, I think it would have. There were key hallmarks of common cryptocurrency investment scams present in the circumstances of Mr U's payments, such as being assisted by a broker and small initial payments which increase in value and frequency.

I've also reviewed the conversations between Mr U and the scammers. I've found nothing within those conversations that suggests Mr U was asked, or agreed to, disregard any warning provided by Revolut. I've also seen no indication that Mr U expressed mistrust of Revolut or financial firms in general. Neither do I think that the conversations demonstrates a closeness of relationship that Revolut would have found difficult to counter through a warning. The weight of evidence that I've outlined persuades me that Mr U was not so taken in by the fraudsters that he wouldn't have listened to the advice of Revolut.

I have seen some evidence that the firm from which the funds used for the scam appear to have originated advised Mr U it no longer facilitated the purchase of cryptocurrency, but I've not seen evidence to suggest it gave further information on why or provided a warning.

Therefore, on the balance of probabilities, had Revolut provided Mr U with an impactful warning that gave details about cryptocurrency investment scams and how he could protect himself from the risk of fraud, I believe it would have resonated with him. He could have paused and looked more closely into the broker before proceeding, as well as making further enquiries into cryptocurrency scams and whether or not the broker was regulated in the UK or abroad. I'm satisfied that a timely warning to Mr U from Revolut would likely have prevented him from making the payment and those that followed.

I'm mindful Revolut spoke with Mr U via its in-app chat and it didn't uncover the scam. I've considered this and find the conversation wasn't good enough. Mr U was asked questions around the circumstances of the investment but I don't think these were open questions which allowed Mr U to explain what happened. Revolut asked if Mr U was purchasing cryptocurrency and that he should use a reputable exchange, when he'd already made many payments to C, a known cryptocurrency exchange, which Revolut was aware of. Given what it knew about the payments at this point I'd have expected Revolut to have asked Mr U a series of open questions about the investment opportunity to try to establish what, if any, scam risk there was. Based on the answers Mr U gave; I'd have expected Revolut to provide a tailored warning highlighting the key features of the scam Mr U was likely falling victim to. Revolut didn't do that here; it didn't ask Mr U open questions regarding the payments he'd made to C. So I don't think it can be reasoned that because the conversation Revolut had

with Mr U on 20 June 2023 didn't prevent him making further payments, that a warning as I've described above, when payment 7 was made, wouldn't have resonated with Mr U.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr U purchased cryptocurrency which credited an e-wallet held in his own name, rather than making a payment directly to the scammers. So, he remained in control of his money after he made the payments from his Revolut account, and it took further steps before the money was lost to the scammers.

I have carefully considered Revolut's view that in a multi-stage fraud, a complaint should be properly considered only against either the firm that is a) the 'point of loss' – the last point at which the money (or cryptocurrency) remains under the victim's control; or b) the origin of the funds – that is the account in which the funds were prior to the scam commencing. It says it is (in this case and others) merely an intermediate link – being neither the origin of the funds nor the point of loss and it is therefore irrational to hold it responsible for any loss.

In reaching my decision, I have taken into account that payment 7 was made to another financial business (a cryptocurrency provider) and that the payments that funded the scam were made from another account at a regulated financial business.

But as I've set out above, I think that Revolut still should have recognised that Mr U might have been at risk of financial harm from fraud when he made payment 7, and in those circumstances it should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it would have prevented the losses Mr U suffered. The fact that the money used to fund the scam came from elsewhere and/or wasn't lost at the point it was transferred to Mr U's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr U's loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

The funds Mr U lost as a result of the scam originated from a firm other than Revolut before being transferred to Mr U's Revolut account, then to purchase cryptocurrency before being sent on to the scammer. I have nothing to suggest the firm intervened when Mr U made payments to his Revolut account.

Ultimately, I must consider the complaint that has been referred to me and for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Mr U's loss from payment 7 (subject to a deduction for Mr U's own contribution which I will consider below).

Should Mr U bear any responsibility for his losses?

In considering this point, I've taken into account what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.

I recognise that, as a layman, there were aspects to the scam that would have appeared convincing. Mr U was already investing with B when he was contacted by the scammer who appeared to be somewhat affiliated with B. The group chat along with the appearance of more than one broker/trader points to this being a persuasive and sophisticated scam.

So I've taken all of that into account when deciding whether it would be fair for the reimbursement due to Mr U to be reduced. I think it should.

Mr U says he carried out checks in to the supposed investment company prior to investing, and I'm persuaded he did some research at the outset.

I've reviewed the conversations between Mr U and the scammer and can see prior to making payment 7 Mr U had some concerns having believed he'd been hacked. He says the funds disappeared before his eyes but the scammer reassures him there's no problem.

I also think Mr U should have been concerned by the promise of stable daily earnings and daily returns of up to 6%. I think Mr U should have recognised that the offer in relation to volatile financial markets was simply too good to be true.

I also think Mr U ought to have been concerned that having supposedly been contacted because he was a customer of B and the investment opportunity appeared to be affiliated with B, he was directed to make payments to C - a competitor of B. I think this should, despite the overall plausibility of the scam, put him on notice that the investment might not be genuine.

I recognise that Mr U 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 these scams. But I have to balance that against the role that Revolut, an EMI subject to a range of regulatory and other standards, played in failing to effectively intervene with a relevant warning. Mr U was taken in by cruel scammers – he was tricked into a course of action by scammers and his actions must be seen in that light. I do not 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 due to an investment scam, 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.

I've concluded, on balance, that Revolut can fairly reduce the amount it pays to Mr U for the recovery scam of his role in what happened. Weighing the fault that I've found on both sides, I think a fair reduction is 50%.

Recovery

I've thought about whether there's anything else Revolut could have done to help Mr U — including if it took the steps it should have once it was aware that the payments were the result of fraud.

Mr U's transfers were to purchase cryptocurrency. In that case the money would have been exchanged into cryptocurrency and sent on to the wallet Mr U gave. It seems that Mr U got the cryptocurrency he paid for and in these cases, there's no real prospect of successful recovery of funds.

My provisional decision

My provisional decision is that Revolut Ltd should pay:

- 50% of Mr U's losses for payment 7 and those that followed – I calculate this to be £17,212.50.
- Pay 8% simple interest per year on this amount, from the date the payments debited his account, until the date the refund is settled (less any tax lawfully deductible).

Mr U accepted the provisional decision. Revolut confirmed it had nothing further to add.

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.

As neither party had anything else to add following my provisional decision, I see no reason to depart from it.

My final decision

For the reasons explained, I uphold this complaint in part and direct Revolut Ltd to pay Mr U:

- 50% of Mr U's losses for payment 7 and those that followed – I calculate this to be £17,212.50.
- Pay 8% simple interest per year on this amount, from the date the payments debited his account, until the date the refund is settled (less any tax lawfully deductible).

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

Charlotte Mulvihill
Ombudsman