DRN-4997139

The complaint

Mr S is complaining that Revolut Ltd didn't do enough to prevent him from making payments to a cryptocurrency investment scam.

What happened

The circumstances of the scam are known to both parties so I won't go into detail here.

In short, around May 2023 Mr S fell victim to a cryptocurrency investment scam, after seeing an advert on social media which appeared to be endorsed by a public figure.

Mr S opened a new account with Revolut, and made payments from his current account with another business to Revolut, and then on to a cryptocurrency exchange – from where the funds were sent to the scam. All of the payments were made to the same cryptocurrency exchange, by debit card.

Payment number	Payment date	Payment amount
1	5 May 2023	£1,000
2	5 May 2023	£1,995
3	8 May 2023	£1,000
4	8 May 2023	£2,000
5	9 May 2023	£3,000
6	11 May 2023	£3,000
7	12 May 2023	£500
8	12 May 2023	£1,000
9	12 May 2023	£1,000
10	12 May 2023	£500
11	18 May 2023	£3,000
12	19 May 2023	£3,000
13	22 May 2023	£1,500

Mr S says he realised he'd been scammed when he attempted to make a withdrawal, but the scammers stopped replying to him. He did have some further conversation with them in November 2023 about getting his money back, and after this he contacted a professional representative to raise a complaint with Revolut.

Revolut replied to say it would raise chargebacks on the payments Mr S made – but it then told him that it was too late to raise them.

Mr S brought his complaint to the Financial Ombudsman and our Investigator looked into what had happened. She thought that Revolut ought to have identified a scam risk to Mr S when he attempted to make Payment 4 and should have given him a written warning highlighting the key features of cryptocurrency investment scams. She thought if Revolut had done this, it would have prevented Mr S from making any further payments to the scam. So, she asked Revolut to refund Mr S's payments to the scam from Payment 4 onwards – with a 50% deduction to reflect Mr S's own liability for his loss.

Mr S accepted the Investigator's findings. But Revolut didn't accept. It said, in summary:

- It would not be required to reimburse 'self-to-self' transactions even if it were a signatory to the Lending Standards Board's Contingent Reimbursement Model Code ("CRM Code").

- The Payment Service Regulator's ("PSR") mandatory reimbursement scheme would not require it to refund payments made in these circumstances either.

- 'Self-to-self' payments don't meet either the Dispute Resolution Rules ("DISP Rules") or CRM Code definition of an APP scam.

- Mr S's loss did not take place from his Revolut account as he made payments to his own account at a cryptocurrency exchange before transferring that cryptocurrency to the fraudster. It's unfair and irrational to hold Revolut responsible for any of the loss where it is only an intermediate link in a chain of transactions. Other firms will have a better understanding of the destination of the funds and/or Mr S's finances and account activity.

Mr S's complaint has now been passed to me for review and a decision.

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.
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 S modified the starting position described in *Philipp,* by – among other things – 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 terms of its contract to refuse payments in certain circumstances, including to comply with regulatory requirements such as the Financial Conduct Authority's Principle for Businesses 6, which required financial services firms to pay due regard to the interests of their customers and treat them fairly. I am satisfied that paying due regard to the interests of its customers and treating them fairly meant Revolut should have been on the look-out for the possibility of fraud and refused card payments in some circumstances to carry out further checks.

In practice Revolut did in some instances refuse or delay payments at the time where it suspected its customer might be at risk of falling victim to a scam.

I must also take into account that the basis on which I am required to decide complaints is broader than the simple application of contractual terms and the regulatory requirements referenced in those contractual terms. I must determine the complaint by reference to what is, in my opinion, fair and reasonable in all the circumstances of the case (DISP 3.6.1R) taking into account the considerations set out at DISP 3.6.4R.

Whilst the relevant regulations and law (including the law of contract) are both things I must take into account in deciding this complaint, I'm also obliged to take into account regulator's guidance and standards, relevant codes of practice and, where appropriate, what I consider to have been good industry practice at the relevant time: see DISP 3.6.4R. So, in addition to taking into account the legal position created by Revolut's standard contractual terms, I also must have regard to these other matters in reaching my decision.

Looking at what is fair and reasonable on the basis set out at DISP 3.6.4R, I consider that Revolut should in May 2023 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.

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 did in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;[1]

[1] 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_/

- 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.

For example, it is my understanding that in May 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat).

I am also mindful that:

- 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)[2].
- 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[3], 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

[2] 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.
[3] BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

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.

- The main card networks, Visa and Mastercard, don't allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain restrictions on their card issuers' right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of transaction, such as by location. The network rules did not, however, prevent card issuers from declining particular payment instructions from a customer, based on a perceived risk of fraud that arose from that customer's pattern of usage. So it was open to Revolut to decline card payments where it suspected fraud, as indeed Revolut does in practice (see above).

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 May 2023 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (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.

Whilst I am required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I am satisfied that to comply with the regulatory requirements that were in place in May 2023, Revolut should in any event have taken these steps.

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

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

Whilst I have set out the circumstances which led Mr S 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 S might be the victim of a scam.

By May 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[4]. And by May 2023, when these payments took place, further restrictions were in place[5].

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 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 S made in May 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 (under the Consumer Duty or otherwise), 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 May 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 (including the Consumer Duty), 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.

---

[4] 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.

[5] In March 2023, Both Nationwide and HSBC introduced similar restrictions to those introduced by Santander in November 2022

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 S'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 S might be at a heightened risk of fraud that merited its intervention.

Mr S's Revolut account was opened as a result of the scam, so it had no account history with which to compare the transactions he was making. This means Revolut would have been relying on generic indicators of fraud risk when the scam payments were made as it would have had no idea of what might be normal for Mr S's account at that time.

I think Revolut should have identified that Payments 1 to 3 were going to a cryptocurrency provider (the merchant is a well-known cryptocurrency provider), but they were not individually of a high value, and I don't think Revolut should reasonably have suspected that they might be part of a scam.

But by the time Payment 4 was made I agree with the Investigator that Revolut ought to have had concerns about what was happening. Payment 4 was made within three minutes of Payment 3, and although not of a particularly high value itself, it took the total value of the payments made to the cryptocurrency exchange on that day to £3,000. Given what Revolut knew about the destination of the payments, and the account activity up to that point, I think that the circumstances should have led Revolut to consider that Mr S was at heightened risk of financial harm from fraud.

In line with good industry practice and regulatory requirements (in particular the Consumer Duty), I am satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this payment went ahead.

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 a warning.

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 May 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 S?

Revolut says it did intervene on an earlier payment of £100 which Mr S attempted to the cryptocurrency provider, by initially declining the payment and freezing Mr S's card. It's

shown us that he would have had to confirm he recognised the payment before his card was unfrozen. When Mr S confirmed he did recognise the payment, it showed him a warning which said:

"Beware of scammers. If someone is claiming to be from Revolut and telling you to do this, cease all contact and terminate the card."

While I don't discount this warning entirely, it is very general in nature and it's difficult to see how it would resonate with Mr S or the specific circumstances of the scam he was experiencing. And I don't think that providing the warning above in relation to an earlier attempted payment was a proportionate or sufficiently specific way to deal with the risk that Payment 4 presented. So, I think Revolut needed to do more.

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 these payments were made.

Taking that into account, I think Revolut ought, when Mr S attempted to make Payment 4, knowing 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 scam, 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. In the warning Revolut ought fairly and reasonably to 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.

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 S 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 S suffered from Payment 4?

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 the balance of probabilities, I think it would have. There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Mr S's payments, such as finding the investment through an advertisement endorsed by a public figure, being assisted by a "broker" and being asked to download remote access software.

I've also reviewed the messaging app and email conversations between Mr S and the scammers. I recognise that some phone calls also take place and I don't know exactly was discussed during these. But I've not found anything within those conversations that suggests Mr S was asked, or agreed to, disregard any warnings Revolut may have provided. I've also

seen no indication that Mr S expressed mistrust of Revolut or financial firms in general. And I don't think that the conversation demonstrates that Mr S had such a close relationship with the scammers, or was so taken in by the scam, that he wouldn't have heeded a warning from Revolut.

I've also seen no evidence that Mr S was provided with warnings by the firm from which the funds used for the scam appear to have originated.

Therefore, on the balance of probabilities, had Revolut provided Mr S 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 circumstances before proceeding, as well as making further enquiries into cryptocurrency scams.

I'm satisfied that a timely warning to Mr S from Revolut would likely have revealed the scam and prevented his further losses.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr S purchased cryptocurrency which credited an e-wallet held in his own name, rather than making a payment directly to the fraudsters. 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 fraudsters.

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 the payments were made to another financial business (a cryptocurrency exchange) and that the payments that funded the scam were made from another account at a regulated financial business.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr S might have been at risk of financial harm from fraud when he made Payment 4 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 loss Mr S 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 S's own account does not alter that fact and I think Revolut can fairly be held responsible for his 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.

I've also considered that Mr S has only complained against Revolut. I accept that it's *possible* that other firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, and Mr S could instead, or in addition, have sought to complain against those firms. But Mr S has not chosen to do that and ultimately, I cannot compel him to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce a consumer's compensation in circumstances where: the consumer has only complained about one respondent from which they are entitled to recover their losses in full; has not complained against the other firm (and

so is unlikely to recover any amounts apportioned to that firm); and where it is appropriate to hold a business such as Revolut responsible (that could have prevented the loss and is responsible for failing to do so). That isn't, to my mind, wrong in law or irrational but reflects the facts of the case and my view of the fair and reasonable position.

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be 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 S's loss from Payment 4 (subject to a deduction for Mr S's own contribution which I will consider below).

Should Mr S 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 note that Mr S has accepted the Investigator's findings on this point, so I won't go into detail here, apart from to say I agree with the Investigator's findings for the following reasons:

- Before he made any payments to the scam Mr S allowed the scammers to use remote access software to help set up his account with Revolut and the cryptocurrency exchange, and I think should have had some concerns about why he was being asked to do this by what he considered to be a legitimate investment company, and whether he was exercising a reasonable degree of caution in allowing a third party access to his devices.

- While I do understand these sorts of social media advertised scams can appear convincing at the outset, at the time Mr S made these payments there was information available online about the company Mr S thought he was dealing with, and about the social media advert for the investment opportunity (including information and advice from the public figure involved) which indicated that it was very likely to be a scam. And I do think that by the time Mr S began to invest in the scam, which was a few weeks after his initial contact with the scammer, and after he'd been asked to give remote access to his devices, he should reasonably have had some time to reflect on the investment opportunity and what had happened so far, which should have prompted further research. And if Mr S had done some research, I can see there was quite a lot of information online at the time to suggest that this particular company and investment scenario may not be legitimate.

- Mr S took out a loan to fund the scam and he's told us the reason he gave for the borrowing was property repairs. I think he ought to have had some concerns about whether a genuine investment company would tell him to take out a loan to a fund an investment, and encourage him to provide an inaccurate reason for why he needed the loan, which again, should have prompted him to look into things further at that point.

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

I do not think however, that the deduction made to the amount reimbursed to Mr S should be greater than 50% taking into account all the circumstances of this case. I recognise that Mr S 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 scam. 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 intervene. Mr S 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 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, 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.

Interest

I've mentioned that Mr S took out a loan to partly fund the payments he made to the scam, and Mr S's representative has told us he is still repaying the full amount he's borrowed, with interest, to the lender. I've thought about this but in all the circumstances, I still think our usual approach of applying 8% simple interest per year to the amount of the refund for Mr S's loss of use of the funds gives a fair and reasonable outcome here.

My final decision

My final decision is that I'm upholding this complaint in part, for the reasons I've explained.

To put things right Revolut Ltd should pay Mr S:

- 50% of the payments he made to the scam, from and including Payment 4, which I've calculated to be £9,250.

- 8% simple interest per annum from the date of the payments to the date of settlement (less any tax lawfully deductible.)

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 12 June 2025.

Helen Sutcliffe
Ombudsman