

## The complaint

Mr U complains that Revolut Ltd didn't do enough to protect him when he was falling victim to a scam, and that it hasn't refunded his losses since the scam was revealed.

## What happened

I issued a provisional decision (PD) for Mr U's complaint on 15 May 2025. I've included a copy of it in this final decision, set out in *italics*.

In it I set out the background to the complaint and so I won't repeat that here. Instead, I'll explain what has happened since the PD.

Mr U let us know that he accepted the findings set out in the PD.

Revolut responded to say it had nothing further to add, and that it would await the final decision. But, as it didn't accept the findings, it is now necessary for me to issue the final decision.

## My provisional findings

*Mr U has said he was approached about a cryptocurrency investment in May 2023. He didn't know at the time, but he'd been contacted by a scammer.*

*The scammer assured Mr U they could help with cryptocurrency investment, which Mr U had some experience of. The scammer told Mr U he could make good profits by using their system.*

*Mr U agreed to sign up and registered for a trading account at the scammer's instruction. The account and platform that hosted it were fake, but Mr U has said they appeared completely genuine.*

*To fund his trading account, Mr U sent a mix existing crypto assets he held and money from his Revolut account. The funds were sent to a cryptocurrency wallet, before being transferred at the scammer's instruction, at which point they were lost. The following payments were made using Mr U's debit card:*

<i>Date</i>	<i>Time</i>	<i>Amount</i>
<i>11 May 2023</i>	<i>18:49</i>	<i>£5,000</i>
<i>15 May 2023</i>	<i>16:04</i>	<i>£5,000</i>
<i>18 May 2023</i>	<i>16:39</i>	<i>£5,000</i>
<i>18 May 2023</i>	<i>16:40</i>	<i>£1,000</i>

*Mr U thought he was making profits, as that's what was showing on his trading account. But when he tried to withdraw, he was told he would have to pay fees. He did so, but still no withdrawal was forthcoming. Mr U was told his withdrawal had been lost in the blockchain and would need recovering, at a cost of £12,000. It was then Mr U realised he'd been the victim of a scam.*

*He reported what happened to Revolut, asking it to help recover his money. Revolut considered whether it could recover the payments through the chargeback process but determined that wasn't possible. And it then concluded there was no other way it could recover the funds, and that Mr U was to be held responsible for the loss.*

*Mr U was unhappy with Revolut's answer and referred his complaint to our service. One of our investigator's considered the complaint and recommended it be upheld.*

*He recognised Mr U had authorised the payments himself, and that they'd gone to a cryptocurrency wallet in his own name before being lost. But he felt the first payment ought to have presented as a risk of financial harm and Revolut ought to have reacted by providing Mr U a warning about cryptocurrency investment scams.*

*Our investigator was satisfied that had Revolut provided such a warning Mr U would have taken notice and stopped what he was doing, thus avoiding the loss. And so he recommended Revolut refund Mr U.*

*He did also say Mr U ought to bear equal responsibility for the final two payments, given they were for fees and charges that had never been explained to Mr U before. He went on to say that, had Mr U carried out some research around what he was being told and the circumstances he was in, he'd likely have uncovered the scam.*

*Mr U accepted the investigator's findings, but Revolut did not. Its overall argument being that Mr U authorised the payments himself, that it had a duty to execute the payment instructions, and that Mr U had paid one of his own accounts meaning the loss occurred outside of the Revolut account.*

*As an agreement hasn't been reached, the complaint has been passed to me to make a decision.*

### ***What I've provisionally 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.*

*Having done so I'm upholding the complaint. But my findings are different to those recommended by our investigator, and I intend to make a lower award of compensation. I'll explain why.*

*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 – 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” (section 20).*

*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;<sup>1</sup>*
- 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*

---

<sup>1</sup> 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/](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/)

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)<sup>2</sup>.*
- *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<sup>3</sup>, 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.*
- *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*

---

<sup>2</sup> Since 31 May 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.

<sup>3</sup> BSI: PAS 17271: 2017” Protecting customers from financial harm as result of fraud or financial abuse”

*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 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 he made by transfers to third parties and to his cryptocurrency wallet (from where that cryptocurrency was 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 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 U might be the victim of a scam.*

*I'm aware that cryptocurrency exchanges like the one used by Mr U generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. Revolut would likely have been aware of this fact too.*

*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. And by May 2023, when these payments took place, further restrictions were in place. 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 U 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.*

*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 on to 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.*

*I think Revolut should have identified that all payments were going to a cryptocurrency provider (the merchant is a well-known cryptocurrency provider). And the very first payment was of a significant value, at £5,000. That is a sum far in excess of any other transactions out of Mr U's account in the previous twelve months, excepting payments to what looks to be another current account in Mr U's name which was a long-established payee, and so I don't find adds much to the considerations here.*

*I have taken account of the fact there had been other crypto activity on Mr U's account, with fiat currency converted in crypto within Revolut. But that is a different form of activity to the transactions in question, and I'd expect Revolut to remain alive to concerns about fiat*

*currency payments to cryptocurrency platforms, especially when they are for as much as the first payment.*

*It's also true Mr U had past transactions to cryptocurrency platforms and a broader platform which allowed for stocks and shares trading. But this activity long pre-dated the scam payments, so I don't see it would be fair and reasonable to consider those in a risk assessment here.*

*In line with good industry practice and regulatory requirements, I am satisfied that it is fair and reasonable to conclude that Revolut should have warned Mr U before the first 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 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 U?*

*Revolut has presented no evidence to suggest any warnings were given to Mr U at any time.*

*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.*

*Taking that into account, I think Revolut ought, when Mr U attempted to make the first payment, knowing (or strongly suspecting) 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 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.*

*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.*

*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.

I also think Revolut's level of concern ought to have escalated when Mr U went to make the second payment, considering it was a further £5,000 sent very shortly after the first. And in those circumstances, it ought to have paused the payment and directed Mr U to the in-app chat to discuss it. I'll not go on to comment on the intervention that ought to have happened here, given the first is enough to establish an error on Revolut's part. But this was a further failing.

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

It is the case that Mr U was in regular contact with the scammer and clearly trusted what he was being told. However, at that stage he'd had no scam education and didn't know what the features of a cryptocurrency investment scam were.

Had those features been clearly set out for him he would have seen that they reflected the very circumstances he was in. I'm satisfied that would have been powerful and would have made Mr U question what he was doing.

I've seen little evidence to suggest Mr U was encouraged to lie to Revolut about why he was making payments. There was no suggestion that he should mislead it if asked, or to ignore warning it gave. And so it follows that he would more likely than not have been honest. And it's more likely than not the delivery of a prominent and impactful warning would have broken the scammer's spell.

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 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 the 'point of loss' – the last point at which the money (or cryptocurrency) remains under the victim's control. It says it is (in this case and others) merely an intermediate link; not 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 each payment was made to another financial business (a cryptocurrency exchange). But as I've set out in some detail above, I think that Revolut still should have recognised that Mr U might have been at risk of financial harm from fraud when they made the first payment, and in those circumstances it should have provided Mr U with a tailored scam warning. If it had taken those steps, I am satisfied it would have prevented the losses Mr U suffered. The fact that the money 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.

I've also considered that Mr U 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 U could instead, or in addition, have sought to complain against those firms. But Mr U has not chosen to do that and ultimately, I cannot compel them to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mr U's compensation in circumstances where: the Mr U 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 U's loss from the first payment (subject to a deduction for Mr U's own contribution which I will consider below).

#### Should Mr U bear any responsibility for their losses?

It is here where my findings differ from those of our investigator. He found that a deduction to Mr U's reimbursement ought only apply to the final two payments. But I'm satisfied it should apply to all payments made.

It's unclear exactly how Mr U came across the supposed investment opportunity and broker. He's said he 'was approached', but I'm not sure what he means by that. Judging by the messages he received, and given what often happens in scams of this nature, it appears likely Mr U interacted with an advert or social media post online and was subsequently contacted. There's nothing to suggest a particularly elaborate setup to the scam.

It then seems to be the case that Mr U would have had little idea of who he was dealing with. And yet, from looking at the messages, it took very little to persuade him to start investing. And he clearly put in a lot of assets very quickly, without doing much to check on the legitimacy of the proposal.

Mr U has said he checked online and could find no negative information about the company. Our investigator said the same. But, when I've looked, that seems to be because there's almost no information at all. And I don't find it would be fair and reasonable to take a complete absence of information as a positive. Not when investing such significant sums of money, being sent to an unknown cryptocurrency wallet/location. Instead, I believe the opposite is true: it ought to have given cause for concern.

One of the few search results that does show up is a company with the same name. But they clearly aren't involved in cryptocurrency trading and yet had the same company logo. So that ought to have caused further concern.

I've also looked at what Mr U was being offered. He was told at different times, before sending any money, that he could expect:

- to make \$1,000 per trade (though there was no indication of how much needed to be invested to make such a return);
- his first trade suggested it would generate an expected profit of 93% within a few minutes.

Within 40 minutes of being told those figures the scammer then explained Mr U could make returns of 300% or 500% in a week, depending on his level of investment.

I consider all of these rates of return to be highly improbable and too good to be true. The proposed returns alone ought to have been viewed with scepticism and caution. But I can't see that Mr U carried out any checks that would have been proportionate to the risk he was being exposed to.

Given these points, I'm satisfied it would be fair and reasonable for Mr U's total reimbursement to be reduced by 50%, so that responsibility for the loss is equally shared.

#### Could Revolut have done anything to recover the funds?

*We know the money went to Mr U's own cryptocurrency wallet and that the funds were quickly moved on to the scammer. This all happened well before the scam was reported. And it means there was no money that could have been returned by the cryptocurrency platform.*

*Whilst a chargeback might be a method sometimes used to see disputed card payments returned to a consumer, there was no prospect of success here. Mr U willingly made the payments himself, and he received the goods and service he contracted for. That is the provision of the wallet services and the supplying of cryptocurrency in exchange for fiat currency. As such there was no right to a chargeback.*

### **Putting things right**

*On Mr U's acceptance, and further to any other information and evidence that might need to be considered, I intend to direct Revolut to:*

- *Refund 50% of the money lost to the scam; and*
- *Pay interest on that sum at 8% simple per year, calculated from the date of loss to the date of settlement.*

### **My provisional decision**

*I intend to uphold this complaint against Revolut Ltd.*

### **What I've decided – and why**

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

I set out my detailed findings in the PD, which can be read above. Since there has been no new argument or evidence put forward by Revolut, and considering Mr U accepted the findings, I see no reason to depart from what I've already said. I uphold the complaint on the same basis as already explained.

### **Putting things right**

On Mr U's confirmed acceptance Revolut must:

- *Refund 50% of the money lost to the scam; and*
- *Pay interest on that sum at 8% simple per year, calculated from the date of loss to the date of settlement.*

### **My final decision**

I uphold this complaint against Revolut Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr U to accept or reject my decision before 20 June 2025.

Ben Murray  
**Ombudsman**