

The complaint

Mr H complains that Revolut Limited won't refund money he lost when he was the victim of a scam.

Mr H is represented by a firm that I'll refer to as 'R'.

What happened

The background to this complaint is well known to both parties and so I'll only refer to some key events here.

In 2023 Mr H fell victim to a task-based job scam. He's explained that, at a time when he was looking for work, he was contacted on an instant messenger application by a recruiter offering him a remote-working job – which we now know to be a scam. The scammer explained that the job with 'E' involved rating products which required simulating their purchase. Mr H was told he could earn 30 – 300 USDT daily, with a basic salary of 700 USDT per week once fully committing to the job continuously for seven days.

Mr H received a link to E's platform for him to set up an account and he was also invited to a group chat with other 'freelancers' in it. The scammer then provided instructions to Mr H on how he could complete the daily tasks – which included funding the account to simulate the purchases. Mr H went on to make the following payments to the scam via a legitimate crypto exchange:

| Transaction date | Type of transaction | Amount |
|------------------|---------------------|----------------|
| 10 May 2023 | Debit card | £1,000 |
| 12 May 2023 | Debit card | £2,000 |
| 12 May 2023 | Debit card | £1,000 |
| 19 May 2023 | Debit card | £10,000 |
| 29 May 2023 | Debit card | £15,700 |
| 8 June 2023 | Debit card | £8,511 |
| 8 June 2023 | Debit card | £160 |
| 13 June 2023 | Debit card | £4,050 |
| 13 June 2023 | Debit card | £30 |
| 19 July 2023 | Debit card | £5,000 |
| 19 July 2023 | Debit card | £6,000 |
| 21 July 2023 | Debit card | £8,000 |
| 21 July 2023 | Debit card | £3,495 |
| 1 August 2023 | Debit card | £9,005 |
| | Total loss: | £73,951 |

Mr H realised he'd been scammed when he was told he had to pay a fee in order to withdraw his funds.

R complained on Mr H's behalf to Revolut on 22 December 2023 saying the payments were made as part of a scam. In short, they said:

- The account activity was out of character and had Revolut intervened in line with industry standards, the scam would've been exposed thereby preventing any further financial loss.
- It is understandable why Mr H felt this job opportunity was real and believable – as he reviewed the website the scammers sent and didn't find anything negative from an internet search. He reviewed the terms and conditions and was also added to an instant messenger group with other freelancers who discussed their lives and jobs.
- The scammers were in constant contact with Mr H, and he was unfamiliar with working from home and this type of work offered. The contact from the scammer also wasn't surprising as he was seeking work at the time.
- Revolut should be on the lookout for this type of scam to prevent their customers from foreseeable harm.
- If Revolut had intervened by asking open probing questions, the scam would've been exposed, and the spell of the scammer would've been broken.
- Mr H was vulnerable at the time of the scam, having been diagnosed with depression and anxiety in which he was taking medication to treat.
- Revolut should refund Mr H and pay 8% simple interest.

Revolut didn't uphold the complaint. In short, they said:

- They raised chargebacks on the transactions to recover the funds lost. But they explained the chargeback process is framed by a very detailed and consistent set of rules. And, essentially, the process includes two types of claims – fraud or dispute – with dispute claims raised for these transactions.
- The outcome of the claims was that they had no right to dispute them as the payments were money orders. And once a money order is processed, the service is considered provided and as described. They're not able to dispute subsequent transactions.

The complaint was referred to the Financial Ombudsman. Our Investigator thought it should be upheld in part. She said Revolut ought to have provided a tailored written scam warning before processing the third payment, but she didn't think this would've made a difference as the warning would've been specific to crypto investment scams (not job scams). But she considered that Revolut ought to have spoken with Mr H before processing the fourth payment (£10,000), which she considered would've allowed Revolut to identify the hallmarks of a job scam – resulting in Mr H not making this or any further payments to it.

Our Investigator thought Mr H should take some responsibility for his loss too. This was because Mr H didn't receive any employment contract and was contacted 'out of the blue'. And the income should've appeared as too good to be true when considering the tasks took little time and effort to complete. Our Investigator also noted that while Mr H says E was a cloned firm and that his research didn't bring up any concerns, she highlighted that the scam website domain was very different to the legitimate firm's website domain – so, she didn't think it would've been easily mistaken. Because of this, our Investigator thought it would be fair for Revolut to refund 50% from the fourth payment onwards and pay 8% simple interest.

R confirmed Mr H's acceptance.

Revolut didn't agree with our Investigator and asked for the matter to be referred to an Ombudsman. In short, Revolut has said:

- This was a 'self-to-self' scenario in which Mr H owned and controlled the beneficiary account to which the payments were sent. Hence, the fraudulent activity didn't occur on Mr H's Revolut account – as the payments were made to a legitimate crypto exchange before being sent to the scam platform.
- The transactions weren't out of character or unexpected with the typical way an electronic money institution (EMI) account is used – particularly as high street banks have started restricting their customers from sending money to crypto exchanges (which is an entirely legitimate activity). Typically, this type of account is opened and used to facilitate payments of a specific purpose and often not used as a main account.
- 'Self-to-self' payments don't meet the Dispute Resolution Rules ("DISP Rules"), nor the Contingent Reimbursement Model (CRM) code or incoming mandatory reimbursement rules definition of an Authorised Push Payment (APP) scam.
- For the Financial Ombudsman to apply the reimbursement rules to self-to-self transactions executed by Revolut is an error in law. Alternatively, the Financial Ombudsman has irrationally failed to consider the fact these transactions are self-to-self and therefore obviously distinguishable from transactions subject to the regulatory regime concerning APP fraud.
- They are also concerned that the Financial Ombudsman appears to have decided as a matter of policy, that Revolut should be left "holding the baby" because, subsequent to the self-to-self transfers involving a Revolut account, customers have transferred those funds to their account with a third party.
- It is entirely relevant to consider possible other bank interventions – as the funds originated from Mr H's own external bank account. As such, they believe it should be considered by the Financial Ombudsman in tandem with this complaint. At the very least, whether Mr H was warned by his external bank is relevant to whether he acted negligently in disregarding any such warnings.
- It might be appropriate for the Financial Ombudsman to exercise its powers under DISP to inform Mr H that it could be appropriate to make a complaint against another firm if necessary.
- The recent reliance by this service on R (on the application of Portal Financial Services LLP) v FOS [2022] EWHC 710 (Admin) is misconceived and amounts to a legal error.
- While they recognise the Financial Ombudsman may have considerable sympathy for customers who have been defrauded, this allocation of responsibility is at odds with the approach the statutory regulator deems appropriate and is irrational.
- It is irrational (and illogical) to hold Revolut liable for customer losses in circumstances where Revolut is merely an intermediate link, and there are typically other financial institutions in the payment chain that have comparatively greater data on the customer than Revolut, but which the Financial Ombudsman hasn't held responsible in the same way as Revolut.

The matter has been passed to me to decide.

Before I proceed to make my final decision, and as our Investigator explained in her assessment, Mr H has confirmed that four payments that he made after the disputed payments listed above were in relation to a different scam. And so, while these were included in R's complaint submission to Revolut, I won't be considering the four payments as part of this complaint. This is because Revolut wasn't given the true circumstances surrounding the payments for them to be fairly considered. Mr H therefore, if he wishes, should complain to Revolut separately about these payments and refer the matter to the Financial Ombudsman if he remains unhappy with their final response.

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 EMI such as Revolut is expected to process payments and withdrawals that a customer authorises them 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, they must carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risk of their 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 their consumer's instructions where they 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 H 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 their 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 their 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 they suspected their 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;
- 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 they identified a scam risk associated with a card payment through their automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through their 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).
- Over the years, the FCA, and their 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 their customer's accounts and scrutinise transactions.
- The October 2017, BSI Code, 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 crypto when considering the scams that their 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 crypto 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 crypto 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 they suspected fraud, as indeed Revolut does in practice (see above).

Overall, taking into account relevant law, regulator's 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 their 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 crypto 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 H was at risk of financial harm from fraud?

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

Whilst I have set out the circumstances which led Mr H 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 them upon which to discern whether any of the payments presented an increased risk that Mr H might be the victim of a scam.

I'm aware that crypto exchanges, like the one Mr H made his payments to here, generally stipulate that the card used to purchase crypto 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. So, it could have reasonably assumed that the payments would be credited to a crypto wallet held in Mr H's name.

By May 2023, when these transactions took place, firms like Revolut had been aware of the risk of multi-stage scams involving crypto for some time. Scams involving crypto have increased over time. The FCA and Action Fraud published warnings about crypto scams in mid-2018 and figures published by the latter show that losses suffered to crypto scams have continued to increase since. They reached record levels in 2022. During that time, crypto 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 customers' ability to purchase crypto using their bank accounts or increase friction in relation to crypto 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 crypto 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 (PSPs), many customers who wish to purchase crypto 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 crypto 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 crypto 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 H made in May 2023, Revolut ought fairly and reasonably to have recognised that their customers could be at an increased risk of fraud when using their services to purchase crypto, notwithstanding that the payment would often be made to a crypto wallet in the consumer's own name.

To be clear, I'm not suggesting 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 crypto in May 2023 that, in some circumstances, should have caused Revolut to consider transactions to crypto 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 they processed such payments. And as I have explained Revolut was also required by the terms of their contract to refuse or delay payments where regulatory requirements meant they 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 crypto, I don't think the fact payments in this case were going to an account held in Mr H'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, they ought to have identified that Mr H might be at a heightened risk of fraud that merited their intervention.

While Revolut should've identified the payments were going to a crypto provider, the first two successful payments were relatively low in value and made on separate days. And so, I don't think there would've been enough reason for Revolut to suspect that they might have been made in relation to a scam.

But by the point of the third and fourth payments, the pattern of the payments changed. By the third payment, Mr H had sent £3,000 in two separate transactions in the space of about an hour. And the fourth payment, albeit a week later, was of a significantly greater value (£10,000). These payments were also made on a newly opened account, which can be a potential indicator of fraud. I understand Revolut needs to take an appropriate line between protecting against fraud and not unduly hindering legitimate transactions. But given what Revolut knew about the destination of the payments, I think the circumstances should have led Revolut to consider that Mr H was at a heightened risk of financial harm from fraud. 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 H before these payments went ahead.

To be clear, I do not suggest that Revolut should provide a warning for every payment made to crypto. Instead, as I've explained, I think it was the combination of the value of the payments and the speed at which they were made, on what was a newly opened account, and that the fact it went to a crypto provider which ought to have prompted warnings.

What did Revolut do to warn Mr H?

Revolut has confirmed that 13 of the card payments were authenticated by 3DS authentication system. But there hasn't been anything to show any scam warnings or education were provided to Mr H before the disputed payments were processed. As per above, 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 these 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 H attempted to make the £1,000 payment on 12 May 2023, knowing (or strongly suspecting) that the payment was going to a crypto provider, to have provided a tailored warning that was specifically about the risk of crypto 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 crypto scams, without significantly losing impact. But I think it would've been a proportionate response to the risk the £1,000 payment presented at that time.

So, at this point in time, I think that such a warning should have addressed the key risks and features of the most common crypto scams – crypto 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 crypto 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 H by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

By the point of the fourth payment however, I don’t consider a tailored written warning would’ve been a proportionate response to the identifiable risk – as £10,000 was significantly greater than Mr H had transacted on his account which, as I’ve said, was newly opened. And so, I think a proportionate response to that risk would be for Revolut to have attempted to establish the circumstances surrounding the payment before allowing it to debit Mr H’s account. I think they should have done this by, for example, directing Mr H to their in-app chat to discuss the payment further.

If Revolut had provided a warning of the type described for the third payment, or if they had attempted to establish the circumstances surrounding the fourth payment, would that have prevented the losses Mr H suffered?

I’ve thought carefully about whether such a warning would’ve resonated with Mr H for the third payment, and to the extent whereby he wouldn’t have proceeded with making it. Having done so, I don’t think it would. This is because the most common features of crypto investment scams – which, as per above, I would’ve expected Revolut to have highlighted – wouldn’t have been relevant to Mr H’s circumstances. Mr H wasn’t making the payments for investment purposes, nor had he come across the opportunity through an advertisement on social media. And while there was a third party that had guided him on how to complete the tasks as part of the job, they weren’t acting on his behalf.

It follows that, while I think Revolut ought to have taken additional steps before processing this transaction, I’m not persuaded that even if Revolut had provided a tailored written crypto scam warning that it would’ve deterred Mr H from making the £1,000 payment. Because of this, I don’t think Revolut’s failure to provide such a warning led to Mr H suffering this part of his loss (or that which preceded it).

I do however think that, had Revolut contacted Mr H to establish the circumstances surrounding the fourth payment of £10,000, they would’ve most likely prevented this loss. This is because, I haven’t seen anything to show that he was being told (or that he agreed) to mislead Revolut about the payment if questioned. Nor has Revolut provided anything to evidence Mr H would’ve misled them about the purpose of the payment. I’ve also listened to a call between Mr H and his existing banking provider – which he used to fund his Revolut account – and when questioned about the purpose of a payment, he explained that it was to purchase crypto for the purpose of a job. Unfortunately, the subsequent questioning and warnings provided to Mr H were tailored towards investment and safe account scams that weren’t relevant to his situation. But because of this, I see no reason why Mr B wouldn’t have similarly been open and honest with Revolut about the purpose of the £10,000 payment if questioned about it.

So, had Revolut contacted Mr H to establish the circumstances surrounding the payment as I would’ve expected, then I consider Mr H would’ve likely explained that he was purchasing crypto for work purposes. Revolut ought to have recognised this as a ‘red flag’ and I consider further appropriate probing would’ve most likely uncovered that Mr H had come across this job opportunity through being messaged on an instant messenger application. And that he

was purchasing crypto to send to E's platform for it to be used to complete tasks, which involved simulating the purchasing of items.

From this, Revolut ought to have recognised that Mr H was falling victim to a scam and given him a very clear scam warning. I've no reason to think Mr H wouldn't have been receptive to such advice and so, on balance, I think it would've caused Mr H to have not gone ahead with the payments.

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

In reaching my decision, I have taken into account that this payment was made to another financial business (a crypto exchange) and that it was funded from another account at a regulated financial business held in Mr H's name and control.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr H might have been at risk of financial harm from fraud when he made the third and fourth payments, and in those circumstances, they should have declined the payments and made further enquiries. If they had taken those steps, I am satisfied they would have prevented the loss Mr H suffered from the fourth payment. The fact that the money used to fund the scam came from elsewhere and wasn't lost at the point it was transferred to Mr H's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr H'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 H 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 H could instead, or in addition, have sought to complain against those firms. But Mr H 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.

Revolut has addressed an Administrative Court judgment, which was referred to in a decision on a separate complaint. As I have not referred to or relied on that judgment in reaching my conclusion in relation to the losses for which I consider it fair and reasonable to hold Revolut responsible, I do not intend to comment on it. I note that Revolut says that they have not asked me to analyse how damages would be apportioned in a hypothetical civil action but, rather, they're asking me to consider all of the facts of the case before me when considering what is fair and reasonable, including the role of all the other financial institutions involved.

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 H's loss from the fourth payment onwards (subject to a deduction for Mr H's own contribution which I will consider below). As I have explained, the potential for multi-stage scams, particularly those involving crypto, ought to have been well known to Revolut. And as a matter of good practice and as a step to comply with its regulatory requirements, I consider Revolut should have been on the

look-out for payments presenting an additional scam risk including those involving multi-stage scams.

Furthermore, I'm aware that Revolut has referenced the CRM code and the PSR's reimbursement scheme for APP scams. But Revolut is not a signatory of the CRM code, and these payments wouldn't have been covered by it anyway. Nor would the payments be covered by the PSR's reimbursement scheme – as it wasn't in force when these payments were made, it isn't retrospective, and it doesn't cover card payments. I've therefore not sought to apply either here. I've explained in some detail why I think it's fair and reasonable that Revolut ought to have identified that Mr H may have been at risk of financial harm from fraud and the steps they should have taken before allowing the aforementioned payments to leave his account.

Should Mr H bear any responsibility for his losses?

I've thought about whether Mr H should bear any responsibility for his loss. In doing so, I've considered what the law says about contributory negligence, as well as what I consider to be fair and reasonable in all the circumstances of this complaint including taking into account Mr H's own actions and responsibility for the losses he has suffered.

When considering whether a consumer has contributed to their own loss, I must consider whether the consumer's actions showed a lack of care that goes beyond what we would expect from a reasonable person. I must also be satisfied that the lack of care directly contributed to the individual's losses.

Here, I consider that there were sophisticated aspects to this scam – including, for example, E's platform showing Mr H's funds and them being used to complete the tasks. I'm also mindful that Mr H spoke with the scammers at length, he reviewed the terms and conditions of the job and was also added to what appeared to be a group with other legitimate freelancers undertaking the same work.

I must however also take into account that, while Mr H was looking for work and had signed up with an online job site, he was offered a job opportunity on an instant messenger application from an unknown person. I also haven't seen anything to show that Mr H received a contract of employment before starting the job with E – which I consider a legitimate employer would be expected to provide. And here, Mr H was told that he could expect to earn between 30 – 300 USDT daily, with a basic salary of 700 USDT per week once fully committing to the job continuously for seven days – which I think is an unrealistically high return for completing a relatively simplistic task of rating products. It would therefore have been reasonable to have expected Mr H to have questioned whether the job opportunity was too good to be true.

Furthermore, I think it is reasonable for Mr H to have questioned the legitimacy of the job opportunity given the requirement for him to purchase significant amounts of crypto. Particularly as by the point of the fourth payment this totalled £14,000 in less than two weeks, which was far greater than the amount Mr H was told he would be expected to earn. The concept of simulating purchases ought to have also been seen by Mr H as likely illegitimate. And the fact Mr H had to deposit funds, especially in the form of crypto, ought to have been of particular concern – as it is highly irregular for someone to have to pay to earn money (especially the amount Mr H did) as part of a job.

Because of this, and taking everything into account, I think Mr H ought to have had sufficient reason to suspect that the job opportunity wasn't legitimate. And so, I would've expected Mr H to have taken greater caution before proceeding. This could've included carrying out online research into this type of job online. Or Mr H could've contacted the online job site

he'd signed up with to check the contact he'd received – and the job opportunity - was genuine. If Mr H had done so, then I consider he would've most likely uncovered that he was being scammed – thereby preventing his losses.

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

Could Revolut have done anything to recover Mr H's money?

The payments were made by card to a legitimate crypto exchange. Mr H sent that crypto to the scammers. So, Revolut would not have been able to recover the funds. In addition, I don't consider that a chargeback would have had any prospect of success given there's no dispute that the crypto exchanges provided crypto to Mr H, which he subsequently sent to the scammers.

Putting things right

I think it is fair that Revolut refund Mr H from the fourth payment onwards (less 50% for contributory negligence). They should also add 8% simple interest to the payments to compensate Mr H for his loss of the use of money that he might otherwise have used.

My final decision

My final decision is that I uphold this complaint in part. I direct Revolut Ltd to pay Mr H:

- 50% of his loss from the fourth payment onwards - £34,975.50.
- 8% simple interest, per year, from the date of each payment to the date of settlement less any tax lawfully deductible.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H to accept or reject my decision before 18 April 2025.

Daniel O'Dell
Ombudsman