DRN-4728280

The complaint

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

Mr P 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 P fell victim to a task-based job scam. At a time when Mr P was looking for work, he was contacted by a 'recruiter' on an instant messenger app saying they'd received his application and offered him a remote-working job opportunity. After confirming his interest, Mr P was contacted by the scam firm – which I'll refer to as 'Z'. The scammer explained the job involved optimising apps to improve their rankings, thereby increasing traffic and download rates. And this would be done by performing random tasks through Z's system – three sets of 40 tasks per day – which would take about one hour per day. For this, Mr P *"could earn a base salary of 6100 USDT (£5000)"* plus commission per month.

The scammer then provided instructions to Mr P on how the job worked, which included setting up an account with Z and a crypto wallet. Mr P was then required to deposit funds to his Z account to be used for simulating the purchase of the apps. And so, Mr P made the following payments to the scam via a legitimate crypto exchange:

Date (time)	**Type**	**Amount (inclusive of fees)**
6 June 2023 (19:36)	Debit card	£40
7 June 2023 (10:48)	Debit card	£300
7 June 2023 (12:27)	Debit card	£400
7 June 2023 (12:56)	Debit card	£200
8 June 2023 (10:05)	Debit card	£1,207.37
8 June 2023 (10:06)	Debit card	£40.58
9 June 2023 (10:31)	Debit card	£1,300
9 June 2023 (11:49)	Debit card	£1,800
9 June 2023 (14:50)	Debit card	£4,400
10 June 2023 (07:51)	Debit card	£5,000

10 June 2023 (07:52)	Debit card	£850
	Total	£15,537.95

Mr P realised he'd been scammed when further payments were demanded from him despite completing the task sets as instructed – he also hadn't been told that deposits would be needed for funds to be withdrawn.

Mr P notified Revolut that the payments were made as part of a scam on 11 June 2023. Revolut directed Mr P to submit chargeback claims, but they said they couldn't find any traces of fraudulent activity on Mr P's account and that they'd confirmed the payments were authenticated by him within their app. Because of this, the funds weren't recoverable via the chargeback process.

Unhappy Revolut wouldn't refund the money he'd lost; Mr P raised a complaint. Revolut's position didn't change, and they explained that, as the payments were authenticated through the 3DS system, it wasn't a valid chargeback under the card scheme's rules – which meant they had to reject it. Revolut directed Mr P to contact the relevant authorities if he believed he'd fallen victim to fraud.

R brought Mr P's complaint to the Financial Ombudsman. In short, they said:

- Mr P sent almost £16,000 to a crypto platform in four days without any questions from Revolut about what they might be for. The transactions weren't in-line with the usual behaviour for his account and so, a robust intervention should've taken place.
- Had Revolut provided a sufficient phone intervention, they would've instantly exposed the scam –as warning signs were there - and avoided Mr P's losses
- Revolut should refund Mr P, pay 8% interest and compensation for the distress he's suffered.

Our Investigator thought the complaint should be upheld in part. She thought Revolut ought to have had concerns that Mr P might be at risk of financial harm by the point of the £4,400 payment and taken steps to protect him from it, including providing a meaningful scam warning. Had they done so, she considered Mr P would've taken it on board – thereby resulting in him not making the payment or those that followed. She did however think Mr P should take some responsibility for his loss too. And so, she recommended Revolut refund 50% of the last three payments – along with paying 8% simple interest to Mr P for loss of use of money.

R confirmed Mr P's acceptance. But Revolut didn't agree and, in short, they added:

- Departures from the law must be acknowledged and explained.
  - The jurisdiction of the Financial Ombudsman is to determine complaints in accordance with the Ombudsman's view of what is 'fair and reasonable'. This requires consideration of "*all the circumstances of the case*", including relevant law and regulations, regulators' rules, guidance and standards, codes of practice and (where appropriate) what the Ombudsman considers was good industry practice at the relevant time.
  - Although an Ombudsman is permitted to depart from the law, if they do so they should say so in their decision and explain why.
  - In recent cases, the Financial Ombudsman has incorrectly stated the duty owed by Revolut to their customers who have been the victims of scams, including authorised push payment (APP) fraud and/or has in effect incorrectly applied the

reimbursement rules to transactions which fall outside their scope.

- Revolut does not owe a duty to prevent fraud and scams.
  - Revolut is bound by contract, applicable regulations, and the common law to execute valid payment instructions. This duty is strict and is subject to very limited exceptions.
  - Revolut's Personal Terms set out the terms and conditions of a customer's personal account and its related services and forms a legal agreement. In accordance with these terms, Revolut agrees to execute transfers in accordance with the instructions the customer inputs into the Revolut app.
  - The Payments Services Regulations (PSR) 2017 impose obligations on payment service providers (PSPs) to execute authorised payment transactions.
  - The Financial Ombudsman overstates Revolut's duty to their customers, and errs in law, by stating Revolut should have *"taken additional steps, or made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud"*. Revolut recognises their obligations to put in place adequate procedures to counter the risk that they may be used to further financial crime (and has such systems and controls in place), but that duty is not absolute and doesn't go as far as to require Revolut to detect and prevent all fraud, particularly in the face of authorised customer instructions.
  - The duty to execute valid payment instructions doesn't require the PSP to assess the commercial wisdom or potential for financial loss of a proposed transaction. This point was recognised in the Supreme Court's judgement in *Phillipp v Barclays Bank UK plc*.
- The reimbursement codes and rules don't generally apply.
  - Revolut isn't a signatory of the voluntary Contingent Reimbursement Model (CRM) code. And the mandatory reimbursement rules are not yet in force and so, they should not apply either.
- "Self-to-self" transactions
  - The CRM code and incoming mandatory (at the time of writing) reimbursement rules wouldn't be applicable on these self-to-self transactions.
  - Self-to-self transactions are payments made between accounts over which the customer has control. In this scenario, as per the definition of APP fraud in DISP 2.7, there is no APP fraud as the payments were not being passed to any other person. The payments left Revolut and went to an account held and accessible by the customer at another financial situation
  - It is for this reason that neither the CRM code nor the mandatory reimbursement rules apply to self-to-self transactions. This is not accidental.
  - 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.
  - 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.

- Their fraud detection systems flagged payments as suspicious, with them immediately blocking Mr P's card and all transactions made from it. This includes:
  - An attempted card payment for £40 on 6 June 2023 at 20:35. They then reached out via their app, whereby they informed Mr P it was identified as suspicious, and which required Mr P to confirm the activity was genuine. Mr P did so, thereby unblocking the card and allowing him to make further transactions. As they verified Mr P was making the payments, they didn't see a reason to stop him making them.
  - An attempted card payment for £5,000 on 9 June 2023 at 19:41. They asked Mr P to provide the source of payment, which he did. And so, this allowed his account to be fully operational and for subsequent payments go through.
- The customer sent the funds under the belief they would get them back with profits. And so, this activity falls under the category of being an investment and not related to a job. Their records show they sent an educational email about potential investment scams in May 2023. It contained information on how to spot opportunities that are too good to be true. So, they performed their duties of informing their users of techniques used by scammers. This warning should be considered here as, if Mr P had taken it more seriously, he would've been aware of the obvious red flags.
- It isn't in dispute that Mr P received and approved the 3DS authentication request, and in doing so, instructed Revolut to proceed with the card payment. Their process is wholly in accordance with the requirements of PSR 67(2). It seems illogical to accept that even if a customer was put under pressure and/or to mislead by a fraudster, the clear wording of Revolut's warnings can simply be discounted. Here, Mr P authorised the disputed payments.

The matter has been passed to me to decide.

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 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 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 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 P 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 June 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 June 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, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in June 2023 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;

- 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 June 2023, Revolut should in any event have taken these steps.

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

It isn't in dispute that Mr P 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 P 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 P might be the victim of a scam.

I'm aware that crypto exchanges, like the ones Mr P 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 P's name.

By June 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 customer's 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 June 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 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 P made in June 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase 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 June 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 P'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 P 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 (it is a well-known crypto provider), the first eight transactions were relatively low in value. 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.

The ninth payment, for £4,400, was however significantly greater in value than those that proceeded it – and out of character for Mr P based on his typical account usage, as it was mostly used for low value transactions. Furthermore, by this point, Mr P had made nine payments in a short period of time, less than 72 hours, that were broadly increasing in value (which are known indicators of potential 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 P 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 taken additional steps, or made additional checks, or provided additional warnings, before processing the payment.

What did Revolut do to warn Mr P

Prior to the scam happening, Revolut has said they provided Mr P with an educational email in May 2023 about potential investment scams. Revolut consider this relevant here as they

argue that Mr P was sending the funds for investment purposes, and it wasn't related to a job. While I've considered this, I disagree. This is because, while Mr P was sending the funds for the purpose of receiving a greater return from it, this was under the belief that he was carrying out legitimate work – the completing of tasks – as part of a job with a genuine employer. He wasn't therefore sending the funds to simply invest but rather, he thought it was a requirement to receive the remuneration the scammer told him he would receive. Because of this, having considered the characteristics of investments scams as described in the educational email, even if Mr P had read it, it wouldn't have resonated with him in the circumstances here. In any event, while banks and EMIs should take proactive steps to educate their customers about the risks of scams, this doesn't negate their responsibility to protect customers from the risk of financial harm at the point of a payment request. As per above, I remain of the view that Revolut should have taken additional steps, or made additional checks, or provided additional warnings, before processing the payment.

Revolut has confirmed their fraud detection systems flagged an attempted £40 payment on 6 June 2023 as suspicious. And that they reached out to Mr P to confirm that it was genuine – which he did. They also blocked an attempted £5,000 payment on 9 June 2023 and asked Mr P to provide the source of payment – which, again, he did.

Although Revolut did carry out some checks to verify the authenticity of a payment request, along with complying with their money laundering obligations, these actions weren't focussed on the purpose of the payment or the underlying risks associated with it. I think Revolut needed to do more before processing the £4,400 payment.

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 P attempted to make the £4,400 payment, knowing (or strongly suspecting) that the payment was going to a crypto provider, to have recognised there was a heightened possibility that the transaction was linked to a scam. In line with the good industry practice that I've set out above, I think a proportionate response to that risk would have been for Revolut to have attempted to establish in more detail the circumstances surrounding the payment before allowing it to debit Mr P's account. I think it should have done this by, for example, directing Mr P to their in-app chat to discuss the payment further to establish the circumstances surrounding it.

If Revolut had attempted to establish the circumstances surrounding the final payment, would that have prevented the losses Mr P suffered?

I've no reason to think Mr P wouldn't have been open or honest with Revolut about the purpose of the payment. And so, had Revolut contacted Mr P to establish the circumstances surrounding it, I think they would've most likely prevented his loss. This is because I think Mr P 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 probing would've most likely uncovered that Mr P had come across this job opportunity through being messaged on an instant messenger app. And that he was purchasing crypto to send to Z's platform for it to be used to complete tasks, which involved using the funds to optimise apps to improve their rankings.

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

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

I have carefully considered Revolut's view that they are (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.

I have taken into account that the payments were made to another financial business 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 P might have been at risk of financial harm from fraud when he made the £4,400 payment, and in those circumstances, they should have declined the payment and made further enquiries. If they had taken those steps, I am satisfied they would have prevented the loss Mr P 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 P's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr P'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 I'm only considering a complaint 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 P could instead, or in addition, have sought to complain against those firms (and referred to our service). But Mr P has not chosen to do that and ultimately, I cannot compel him to. In these circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mr P's compensation in circumstances where: Mr P has only complained about one respondent from which they are entitled to recover their losses in full; has not complained against the other firm(s) (and so is unlikely to recover any amounts apportioned to that firm(s)); 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 P's loss from the £4,400 payment made on 9 June 2023 (subject to a deduction for Mr P'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 their 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 P may have been at risk of financial harm from

fraud and the steps they should have taken before allowing the £4,400 payment to leave his account.

Should Mr P bear any responsibility for his losses?

I've thought about whether Mr P should bear any responsibility for his loss. In doing so, I've considered what the law says about contributory negligence, as well as what I consider to be fair and reasonable in all of the circumstances of this complaint including taking into account Mr P'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, Z's platform showing Mr P's funds and them being used to complete the tasks. I must however also take into account that, while Mr P was looking for work, he was offered a job opportunity from a recruiter on an instant messenger app. At which point, I should note that I've not seen any evidence to show Mr P submitted his details to the recruitment agency that contacted him (and therefore was expecting contact from them). Nevertheless, I consider being contacted through an instant messenger app as highly unusual – and not the method of contact expected from a legitimate recruitment agency.

I also haven't seen anything to show that Mr P received any contract of employment before starting the job with Z – which, similarly, I would expect to see provided by a legitimate employer. Particularly given Mr P was told that he could expect to earn a base salary of £5,000 per month plus commission – which, I would add, is an unrealistically high return for completing relatively simplistic tasks. It would therefore have been reasonable to have expected Mr P to have questioned whether the job opportunity was too good to be true. Furthermore, I think it is reasonable for Mr P to have questioned the legitimacy of the job opportunity given the requirement for him to purchase significant amounts of crypto in order to simulate the purchase of the apps. The concept of undertaking fake purchases to boost the popularity of apps ought to have been seen by Mr P as likely illegitimate. And the fact Mr P 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 P did) as part of a job.

Because of this, and taking everything into account, I think Mr P ought to have had sufficient reason to suspect that the job opportunity wasn't legitimate. And so, I would've expected Mr P to have taken greater caution before proceeding. This could've included carrying out online research into this type of job online. Or Mr P could've contacted the recruitment firm directly to check the contact he'd received was genuine. If Mr P 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 P in relation to the last three payments 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 P's money?

The payments were made by card to a legitimate crypto exchange. Mr P sent that crypto to the fraudsters. 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 exchange provided crypto to Mr P, which he subsequently sent to the fraudsters.

Putting things right

I think it is fair that Revolut refund 50% of the last three payments Mr P made to the scam – totalling £5,125. They should also add 8% simple interest to the payment to compensate Mr P 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 P:

- £5,125 – that being 50% of the last three payments.
- 8% simple interest, per year, calculated 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 P to accept or reject my decision before 7 February 2025.

Daniel O'Dell
Ombudsman