DRN-5094180

The complaint

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

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

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 I fell victim to a task-based job scam. He was contacted on an instant messenger application by an unknown person who introduced him to a remote-working job – which we now know to be a scam – with a firm I'll refer to as 'A'. The scammer explained the job involved completing 20 tasks per day to help merchants promote their products on A's platform. Mr I was told by the scammer that it took around ten to thirty minutes per day, and that their earnings were usually *"tens to hundreds of pounds in commission every day, but I usually earn tens of pounds"*. It was also explained that, as part of the job, there would be 'lucky orders' which could earn Mr I more commission. But when there wasn't enough account balance to complete these 'lucky orders', topping up of the account was required.

Mr I received a link to A's platform for him to set up an account. The scammer then provided instructions to Mr I on how he could complete the sets – which included funding the account to complete the 'lucky orders' by purchasing crypto. Mr I went on to make the following payments to the scam - via legitimate crypto providers and peer-to-peer crypto purchases:

Transaction date	**Payment method**	**Transaction type**	**Amount**
24 September 2023	Push to card	Peer to Peer	£100
24 September 2023	Push to card	Peer to Peer	£130
27 September 2023	Debit card	Crypto Provider A	£500
27 September 2023	Debit card	Crypto Provider A	£500
27 September 2023	Debit card	Crypto Provider A	£3,000
27 September 2023	Debit card	Crypto Provider A	£4,700
27 September 2023	Fund transfer	Crypto Provider B	£4,700
		Total:	£13,630

Mr I received credits of £16.27 and £420.90 on 25 September 2023, and £1,242.99 on

27 September 2023. This puts his total loss from the scam to £11,949.84.

Mr I realised he'd been scammed when he couldn't withdraw his earnings, and he reported the scam to Revolut on 28 September 2023. C then complained on Mr I's behalf to Revolut on 30 October 2023 saying the payments were made as part of a scam. In short, they said:

- Revolut failed in their duty of care to protect Mr I from the scam. They allowed the payments to leave Mr I's account without carrying out an effective intervention.
- These payments should've been identified by Revolut as unusual – given their value and being made to new payees – and investigated them thoroughly. Had further enquiries happened, such as asking Mr I what the payments were for and the basic surrounding context, Revolut would've become aware he was being scammed and ought to have provided an effective warning. This, in turn, would've prevented the payments being made.
- Mr I had a reasonable basis to believe this scam was genuine – as the scam website looked professional, the firm's social media was consistent throughout and he received withdrawals in the early stages (giving the false impression he could withdraw more). Furthermore, he looked at several reviews which all appeared positive and, as he was looking for a job at the time, the contact from the scammer wasn't unusual.
- To settle this complaint, they said Mr I would accept a full reimbursement of his losses, 8% interest and £300 compensation.

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

- Mr I hadn't yet submitted chargeback claims for the debit card transactions, and so they recommended he do so.
- Upon being notified of the scam, they launched a request to freeze and retrieve the funds from the beneficiary's bank account. The recovery of funds isn't guaranteed.
- Their systems detected the fund transfer was being made to a new beneficiary and provided him warnings – which included a message about the purpose of the payment, followed by educational screens regarding the type of potential scam. Mr I was free to continue with the transactions following these warnings.
- Revolut also frequently informs customers about scam prevention tips.
- Revolut wasn't at fault for processing the transfer that Mr I authorised in the form and procedure agreed in the terms and conditions.
- Revolut isn't liable for these authorised transactions and has treated Mr I fairly.

The complaint was referred to the Financial Ombudsman. Our Investigator thought it should be upheld in part. He thought Revolut could've prevented Mr I's loss from the point of the £3,000 payment had they questioned it appropriately. This would've allowed Revolut to have identified the hallmarks of a job scam, thereby allowing them to provide a warning tailored to that scam risk. Our Investigator did however think Mr I should take some responsibility for his loss too. So, he thought it would be fair for Revolut to refund 50% of the last three payments along with paying 8% simple interest.

C confirmed Mr I's acceptance.

Revolut requested a decision from an Ombudsman. In short, Revolut added:

- This is a 'self-to-self' scenario in which Mr I owned and controlled the beneficiary account to which the majority of payments were sent. Hence, the fraudulent activity didn't occur on Mr I's Revolut account – as the payments were made to legitimate crypto providers before being sent to the scam platform.

- ‘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.
- 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.
- It is entirely relevant to consider possible other bank interventions.
- It might be appropriate for the Financial Ombudsman to exercise their powers under DISP to inform Mr I that it could be appropriate to make a complaint against another firm if necessary.
- 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.

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 deciding what’s fair and reasonable, I am required to take into account relevant law and regulations, regulators’ rules, guidance and standards, and codes of practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

In broad terms, the starting position at law is that an 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, 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 I 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).

In this respect, section 20 of the terms and conditions said:

> *"**20. When we will refuse or delay a payment***
>
> *We must refuse to make a payment or delay a payment (including inbound and outbound payments) in the following circumstances:*
>
> - *If legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks;*
> - *…"*

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

I am satisfied that, to comply with regulatory requirements (including the Financial Conduct Authority's "Consumer Duty", which requires financial services firms to act to deliver good outcomes for their customers) Revolut should in September 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.

So, Revolut's standard contractual terms produced a result that limited the situations where they could delay or refuse a payment – so far as is relevant to this complaint – to those where applicable regulations demanded that they do so, or that they make further checks before proceeding with the payment. In those cases, they became obliged to refuse or delay the payment. And I'm satisfied that those regulatory requirements included adhering to the FCA's Consumer Duty.

The Consumer Duty – as I explain below – requires firms to act to deliver good outcomes for consumers.

Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, Revolut was required act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud. The Consumer Duty is therefore an example of a regulatory requirement that could, by virtue of the express terms of the contract and depending on the circumstances, oblige Revolut to refuse or delay a payment notwithstanding the starting position at law described in Philipp.

I have taken both the starting position at law and the express terms of Revolut's contract into account when deciding what is fair and reasonable. I am also mindful that in practice, whilst their terms and conditions referred to both refusal and delay, the card payment system rules meant that Revolut could not in practice delay a card payment, they could only decline ('refuse') the payment.

But 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 September 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 do 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 September 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).
- Since 31 July 2023, under the FCA's Consumer Duty, regulated firms (like Revolut) must act to deliver good outcomes for customers (Principle 12) and must avoid causing foreseeable harm to retail customers (PRIN 2A.2.8R). Avoiding foreseeable harm includes ensuring all aspects of the design, terms, marketing, sale of and support for their products avoid causing foreseeable harm (PRIN 2A.2.10G). One example of foreseeable harm given by the FCA in their final non-handbook guidance on the application of the duty was *"consumers becoming victims to scams relating to their financial products for example, due to a firm's inadequate systems to detect/prevent scams or inadequate processes to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers"*.
- 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 September 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;
- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of their products, including the contractual terms, enabled them to do so;
- 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 September 2023, Revolut should in any event have taken these steps.

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

It isn't in dispute that Mr I has fallen victim to a cruel scam here, nor that he authorised the payments he made to his crypto wallet (from where that crypto was subsequently transferred to the scammer) – whether directly to the crypto platforms or via peer-to-peer purchases.

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

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

By September 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 September 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 I made in September 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 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 crypto in September 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 (including the Consumer Duty), 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 I'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 I might be at a heightened risk of fraud that merited their intervention.

The first two transactions were of a very low value and, as they were peer-to-peer crypto purchases, they wouldn't have been identifiable as crypto transactions to Revolut. The following two transactions, albeit identifiable as crypto due to being made to a crypto provider, were likewise of a relatively low value. Because of this, 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 £3,000 payment was however for an increased amount, and much higher than Mr I typically spent on his account - as he mostly used it for low value day-to-day transactions. It was also the third payment made to a crypto provider on the same day, and payments made in a short period of time that are increasing incrementally in value is an indicator of potential fraud. There also doesn't appear to have been any prior crypto activity on Mr I's account before these disputed transactions. And so, while I appreciate Revolut needs to take an appropriate line between protecting against fraud and not unduly hindering legitimate transactions, I think this increase in value and change in account usage ought to have been concerning to Revolut. And given what Revolut knew about the destination of the payment, I think the circumstances should have led Revolut to consider that Mr I 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 I before the payment 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 payment and that it out was out of character for Mr I, and that the fact it went to a crypto provider which ought to have prompted a warning.

What did Revolut do to warn Mr I?

In respect of the push to card payments, Mr I was given the following warning:

> *"**Do you know this payee?***
>
> *Never pay someone you don't know or trust.*
>
> *Be careful, as fraudsters can impersonate other people. We'll never ask you to send funds out of your account.*
>
> *If you're unsure, don't make the payment. If this payee turns out to be fraudster, you may lose your money and not be refunded."*

This scam warning was tailored towards safe account scams, which wasn't relevant to Mr I's situation. And given Mr I trusted the scammer and believed the job opportunity to be legitimate, I don't think this would've given him sufficient reason to question the legitimacy of his transactions. Nor raised his awareness that he was likely being scammed.

Revolut has confirmed that the card payments were authorised via 3DS authentication system. But the only additional warnings provided were in relation to the final transaction – which was a £4,700 fund transfer. Revolut has shown that Mr I was shown a warning similar to the above in respect of this transaction. And following this, Mr I was provided a set of dynamic educational story messages to warn him about the risks associated with this payment.

Mr I was also asked about the purpose of his payment, which he selected "goods and services" from the available options. This resulted in Mr I receiving further warning messages based on the stated payment purpose of the transactions. Mr I chose to proceed with making the payment. The warnings he was given however weren't relevant to his circumstances as he was purchasing crypto as part of a job opportunity – and so the warnings around purchase scams, being wary of bargains and asking for proof of ownership wouldn't have given Mr I the knowledge or reason to suspect he might be falling victim to a scam.

As per above, I think Revolut needed to do more before processing the £3,000 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.

As I've set out above, the FCA's Consumer Duty, which was in force at the time these payments were made, requires firms to act to deliver good outcomes for consumers including acting to avoid foreseeable harm. In practice this includes maintaining adequate systems to detect and prevent scams and to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers.

I'm mindful that firms like Revolut have had warnings in place for some time. They, along with other firms, have developed those warnings to recognise both the importance of identifying the specific scam risk in a payment journey and of ensuring that consumers interact with the warning.

In light of the above, I think that by September 2023, when these payments took place, Revolut should have had systems in place to identify, as far as possible, the actual scam that might be taking place and to provide tailored, effective warnings relevant to that scam for both APP and card payments. I understand in relation to Faster Payments they already had systems in place that enabled them to provide warnings in a manner that is very similar to the process I've described.

I accept that any such system relies on the accuracy of any information provided by the customer and cannot reasonably cover off every circumstance. But I consider that by September 2023, on identifying a heightened scam risk, a firm such as Revolut should have taken reasonable steps to attempt to identify the specific scam risk – for example by seeking further information about the nature of the payment to enable them to provide more tailored warnings.

In this case, Revolut knew that the £3,000 payment, and the two that preceded it earlier that day, was being made to a crypto provider and their systems ought to have factored that information into the warning they gave. Revolut should also have been mindful that crypto scams have become increasingly varied over the past few years. Fraudsters have increasingly turned to crypto as their preferred way of receiving victim's money across a range of different scam types, including investment, impersonation and job scams.

Taking that into account, I am satisfied that, by September 2023, Revolut ought to have attempted to narrow down the potential risk further. I'm satisfied that when Mr I made the payment, Revolut should – for example by asking a series of automated questions designed to narrow down the type of crypto related scam risk associated with the payment he was making – have provided a scam warning tailored to the likely crypto related scam Mr I was at risk from.

In this case, Mr I was falling victim to a 'job scam' – he believed he was making payments in order to receive an income.

As such, I'd have expected Revolut to have asked a series of simple questions in order to establish that this was the risk the payment presented. Once that risk had been established, they should have provided a warning which was tailored to that risk and the answers Mr I gave. I'd expect any such warning to have covered off the key features of such a scam, such as making payments to gain employment, being paid for 'clicks', 'likes' or promoting products and having to pay increasingly large sums without being able to withdraw money.

I acknowledge that any such warning relies on the customer answering questions honestly and openly, but I've seen nothing to indicate that Mr I wouldn't have so here. This is because, having reviewed his conversation with the scammer, I haven't seen anything to show he was told – or that he agreed – to mislead Revolut if questioned about the payments. I'm also mindful that Mr I, on the subsequent fund transfer transaction, selected the payment purpose as being for 'goods and services'. The option for 'as part of a job opportunity' wasn't listed on this page but had to be accessed via the 'something else' option. I wouldn't reasonably have expected Mr I to have known this. And considering he was making the payment to acquire and send crypto; I think the option he selected - 'goods and services' - was the most accurate available to him on that page. I therefore think it was reasonable for him to select it.

And so, I think it is fair and reasonable to conclude that Revolut ought to have initially declined the final £3,000 payment in order to make further enquiries and with a view to providing a specific scam warning of the type I've described. Only after that scam warning had been given, if Mr I attempted the payment again, should Revolut have made the payment.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr I suffered from the £3,000 payment onwards?

I've thought carefully about whether such a warning would've resonated with Mr I for the £3,000 payment, and to the extent whereby he wouldn't have proceeded with making it. Having done so, I think it would.

Mr I clearly trusted the scammer and followed their instructions under the belief the job opportunity was legitimate. That said, I'm not persuaded that Mr I was so heavily under the spell whereby he wouldn't have been receptive to relevant and tailored advice and/or scam warnings from Revolut. And from the conversation with the scammer, shortly prior to making the payment, Mr I questions *"Is 3000 not too big".* And so, from this, I think it's reasonable to conclude that Mr I had some nervousness and doubts about the value of the transaction at that time.

Because of this, I think a warning – of the type described – would've very likely resonated with Mr I and been enough to persuade him that he was likely falling victim to a scam.

I haven't seen anything to show Mr I ignored any warnings relevant to his situation. And so, I think Mr I would've most likely heeded such a warning at the point of the £3,000 payment. It follows that I think it would've been enough to have made Mr I realise that the job opportunity wasn't genuine. In turn, I consider it most likely Mr I wouldn't have gone ahead with the £3,000 payment or those that followed.

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

In reaching my decision, I have taken into account that the payments were made other financial businesses (crypto providers) and that they were funded from another account at a regulated financial business held in Mr I's name and control.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr I might have been at risk of financial harm from fraud when he made the £3,000 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 I suffered. 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 I's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr I'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 I 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 I could instead, or in addition, have sought to complain against those firms. But Mr I has not chosen to do that and ultimately, I cannot compel him to. In those circumstances, I can only make an award against Revolut.

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

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

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be referred to me) and for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Mr I's loss from the £3,000 payment onwards (subject to a deduction for Mr I'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, and it isn't retrospective. 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 I may have been at risk of financial harm from fraud and the steps they should have taken before allowing the £3,000 payment to leave his account.

Should Mr I bear any responsibility for his losses?

I've thought about whether Mr I 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 I'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, A's platform showing Mr I's funds used to complete the tasks. I'm also mindful that Mr I has said he was looking for work at the time, and so the contact wasn't unusual or unexpected.

I must however also take into account that, while Mr I says he was actively looking for work, he was offered a job opportunity on an instant messenger application from an unknown person. And despite Mr I asking the scammer how they got his number and whether they'd met before, the scammer replied *"I don't remember"* and asked *"What's your name?"*. I consider this contact ought to have been seen by Mr I as highly suspicious and brought him to question the legitimacy of a job opportunity offered by someone that clearly didn't know him, and so it wouldn't have been as a result of his own job search.

I also haven't seen anything to show Mr I received a contract of employment before starting the job with A – which I consider a legitimate employer would be expected to provide. And here, Mr I was told he could earn daily commission of *"tens to hundreds of pounds"* for only ten to thirty minutes. I think this is an unrealistically high return for completing relatively simplistic tasks. It would therefore have been reasonable to have expected Mr I to have questioned whether the job opportunity was too good to be true. I'd also note that the requirement of having to pay £3,000 was significantly greater than what Mr I was led to

believe he would earn at this point too. And so, this should've been seen as excessive and suspicious.

Furthermore, I think it is reasonable for Mr I to have questioned the legitimacy of the job opportunity given the requirement for him to purchase crypto – and a significant amount at the £3,000 point. The concept of falsely promoting products on A's platform also ought to have been seen by Mr I as likely illegitimate. And the fact Mr I 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 I did) as part of a job.

Because of this, and taking everything into account, I think Mr I ought to have had sufficient reason to suspect that the job opportunity wasn't legitimate. And so, I would've expected Mr I to have taken greater caution before proceeding - and not simply relied on what the scammer told him. This could've included carrying out research into this type of job online. Or Mr I could've contacted the firms he'd interacted with as part of his job search, or his banking provider(s), to query whether this type of employment – and the contact he'd received - was genuine. If Mr I 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 I 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 I's money?

The debit card payments were made to a legitimate crypto provider. I don't consider that chargebacks had any reasonable prospect of success given there's no dispute that Mr I received the service he paid for, that being the crypto which he subsequently sent to the scammers.

In respect of the fund transfer to the crypto provider, Revolut could only contact the beneficiary bank – that being the bank used by the crypto provider. But Mr I moved the funds from his crypto wallet to the scammers. And so, there wouldn't have been any funds remaining for Revolut to recover. And in respect of the crypto purchased via the peer-to-peer market, Revolut wouldn't have had any basis to request the return of those funds as the crypto had been provided.

It follows that I don't think Revolut could reasonably have done anything more to recover Mr I's loss.

Putting things right

I think it is fair that Revolut refund Mr I the last three payments (less 50% for contributory negligence). They should also add 8% simple interest to the payments to compensate Mr I 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 I:

- 50% of the last three payments - £6,200
- 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 I to accept or reject my decision before 1 May 2025.

Daniel O'Dell
Ombudsman