DRN-5008340

The complaint

Mrs T complains that Revolut Ltd won't refund money she lost when she was the victim of a scam.

Mrs T 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 late 2023 Mrs T fell victim to a task-based job scam. She's explained that she was contacted on an instant messenger application offering her a remote-working job – which we now know to be a scam. The scammer said she'd been passed Mrs T's details from a contact at a recruitment firm. And they explained to Mrs T that the job with 'C' involved assisting retailers that had subscribed to their company's service *"to drive their product data value so they can gain more exposure to attract consumers and investors".* This didn't require writing reviews or finding customers to promote or help with sales, but it needed the *"product data distributed by the platform"* to be submitted with a *"single click"*. And it involved the completion of sets of product data. Mrs T was told she would earn daily commission of 50-200 USDT daily, along with a salary based on the number of continuous days worked – 100 USDT after two working days, 500 USDT after five working days and 1,200 USDT after ten working days. Mrs T was told the job would require 30 – 40 minutes of her time each day.

Mrs T received a link to C's platform for her to set up an account and she was also invited to a group chat with other employees. The scammer then provided instructions to Mrs T on how she could complete the sets – which included funding the account to bring it into a positive due to receiving 'merge data' (which consisted of more than one item and would, supposedly, provide a greater profit). Mrs T went on to make the following payments to the scam via legitimate crypto exchanges:

Transaction date	Type of transaction	Amount
30 October 2023	Debit card	£81
30 October 2023	Debit card	£116
2 November 2023	Debit card	£180
2 November 2023	Debit card	£200
2 November 2023	Debit card	£200
2 November 2023	Debit card	£200

3 November 2023	Debit card	£190
3 November 2023	Debit card	£190
3 November 2023	Debit card	£190
3 November 2023	Debit card	£190
3 November 2023	Fund transfer	£1,500
7 November 2023	Debit card	£4,000
7 November 2023	Debit card	£3,450
	Total:	£10,687

Mrs T received a credit from a crypto exchange of £157.17 on 30 October 2023. She also had a transfer refund of £1,500 on 8 November 2023 – which appears to be a refund for the 3 November 2023 transaction.

Mrs T realised she'd been scammed when she was pressurised into making more and higher value payments, as well being encouraged to take out a loan (which she didn't do).

Mrs T notified Revolut that she'd been scammed on 8 November 2023 and was directed to submit chargebacks for the transactions. Revolut attempted recovery and was successful with the four £190 transactions, which was provisionally returned to Mrs T on 9 November 2023.

R complained on Mrs T's behalf to Revolut on 22 November 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 Mrs T felt this job opportunity was real and believable – as she reviewed C's website that was impersonating a legitimate firm. She was also added to an instant messenger group with other employees, and she spoke at length with C's customer service team and other persons within the firm that seemed professional. Mrs T also received comprehensive training on the job role.
- The scammer was in constant contact with Mrs T, and she was unfamiliar with working from home and this type of work offered.
- 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.
- Revolut should refund Mrs T and pay 8% simple interest.

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

- They raised chargebacks on the debit cards 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 fraud claims raised for these transactions.

- The outcome of the claims was that they had no right to dispute them as they'd found no traces of fraudulent activity on Mrs T's account – as they were authorised via 3DS authentication system.
- They noted however that their chargeback team was still investigating the four £190 payments, and that they would update Mrs T further.

The complaint was referred to the Financial Ombudsman. Our Investigator thought it should be upheld in part. She thought Revolut could've prevented Mrs T's loss from the point of the £4,000 payment by asking her a series of questions to establish the surrounding circumstances of the crypto payment, thereby allowing them to provide a warning tailored to that scam risk. Our Investigator did however think Mrs T should take some responsibility for her loss too. So, she thought it would be fair for Revolut to refund 50% of the last two payments along with paying 8% simple interest.

R confirmed Mrs T's acceptance.

Revolut didn't agree with our Investigator and asked for the matter to be referred to an Ombudsman. They didn't consider the £4,000 payment was unusual for Mrs T as, by this point, it was a known merchant – with 13 payments made over an eight-day period. And as they were being made to a well-known crypto merchant, they were going to an account in the customer's own name and so weren't concerning. Because of this, they had no reason to stop or delay the payments.

Our Investigator's view didn't change. She explained that crypto carries a known risk due to the increase in scams with this type of payment. And despite Mrs T having never made crypto payments before, a pattern had developed leading up to the £4,000 payment. This wasn't normal activity for Mrs T's account and the transactions we're increasing in value. And given Revolut's knowledge of multi-stage scams, they should be on the lookout for this type of scam. So, Revolut should've enquired about the £4,000 payment. Had they done so, they would've uncovered the scam.

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

- This is a 'self-to-self' scenario in which Mrs T owned and controlled the beneficiary account to which the payments were sent. Hence, the fraudulent activity didn't occur on Mrs T's Revolut account – as the payments were made to a legitimate crypto exchange 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.
- 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 Mrs T 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 Mrs T 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 Mrs T 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 October 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 October 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 October 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 October 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 October 2023, Revolut should in any event have taken these steps.

Should Revolut have recognised that Mrs T was at risk of financial harm from fraud?

It isn't in dispute that Mrs T has fallen victim to a cruel scam here, nor that she

authorised the payments she made to her crypto wallet (from where that crypto was subsequently transferred to the scammer).

Whilst I have set out the circumstances which led Mrs T to make the payments using her 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 Mrs T might be the victim of a scam.

I'm aware that crypto exchanges, like the one Mrs T made her card payments to here, generally stipulate that the card used to purchase crypto at the 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, they could have reasonably assumed that the payments would be credited to a crypto wallet held in Mrs T's name.

By October 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 October 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 Mrs T made in October 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 October 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 Mrs T'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 Mrs T 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 ten payments were of a very low value - £200 or less. They were also spread over a five-day period 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 next payment, which as I've said appears to have been refunded, was for an increased amount and to a different crypto provider. But despite the increase in value, I don't think this transaction was so unusual or suspicious for Revolut to have been concerned. This is because, while Mrs T's account was typically used for low value day to day transactions, it's not uncommon for consumers to make occasional higher value payments at times.

The £4,000 payment was however much greater than those that preceded it, and it was significantly out of character with how Mrs T typically used her account. This is because, as I've said, she typically used it for low value day to day transactions, and there also doesn't appear to have been any prior crypto activity on her account before 30 October 2023. 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 Mrs T 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 Mrs T 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 Mrs T, and that the fact it went to a crypto provider which ought to have prompted a warning.

What did Revolut do to warn Mrs T?

Revolut has confirmed the payments were authorised via 3DS authentication system but haven't shown that they provided any scam warnings to Mrs T before processing the payments.

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 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 October 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 October 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 payment(s) 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 October 2023, Revolut ought to have attempted to narrow down the potential risk further. I'm satisfied that when Mrs T 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 she was making – have provided a scam warning tailored to the likely crypto related scam Mrs T was at risk from.

In this case, Mrs T was falling victim to a 'job scam' – she believed she 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 Mrs T gave. I'd expect any such warning to have covered off 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 Mrs T wouldn't have done so here – as

there wasn't any interaction with Revolut, nor with her bank that she used to fund the payments. There also isn't anything within the chat with the scammer to show Miss T was told, or that she agreed, to mislead Revolut if questioned about the payment(s).

And so, I think it is fair and reasonable to conclude that Revolut ought to have initially declined the final £4,000 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 Mrs T 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 Mrs T suffered from the £4,000 payment onwards?

I've thought carefully about whether such a warning would've resonated with Mrs T for the £4,000 payment, and to the extent whereby she wouldn't have proceeded with making it. Having done so, I think it would.

I've read the instant message conversation between Mrs T and the scammer. And at the outset, Mrs T questions where her details were obtained from, as she didn't want it to be some *"sort of scam"*. The scammer told Mrs T that she'd obtained them from a person at a recruitment firm and reassured her that she'd been doing it for several months and nothing had ever happened. This, to me, suggests that Mrs T had some concerns from the outset regarding the initial contact she received.

A few days prior to the £4,000 payment, Mrs T also told the scammer that she just wanted to stop and get her money back at the least. Despite the scammer reassuring her she'd get all her money back when she completed the data set, Mrs T explained that she didn't have any more funds for the next seven days. And she reiterated that she didn't want to continue but asked if she could please get her money back, along with asking if the scammer could assist. Mrs T made it clear that she only needed her money back, but her 'pay' could be kept.

From this, I think Mrs T was clearly extremely worried about her financial position and showed signs of desperation in trying to recover what she'd already paid towards the scam. Because of this, I think a warning – of the type described – would've very likely resonated with Mrs T and been enough to persuade her that she was likely falling victim to a scam.

I haven't seen anything to show Mrs T ignored any warnings relevant to her situation. And so, I think Mrs T would've most likely heeded such a warning at the point of the £4,000 payment. It follows that I think it would've been enough to have made Mrs T realise that the job opportunity wasn't genuine. In turn, I consider it most likely Mrs T wouldn't have gone ahead with the £4,000 payment (or the £3,450 payment that followed).

Is it fair and reasonable for Revolut to be held responsible for Mrs T'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 Mrs T's name and control.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mrs T might have been at risk of financial harm from fraud when she made the £4,000 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 Mrs T 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 Mrs T's own account does not alter that fact

and I think Revolut can fairly be held responsible for Mrs T'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 Mrs T 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 Mrs T could instead, or in addition, have sought to complain against those firms. But Mrs T has not chosen to do that and ultimately, I cannot compel her 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 Mrs T's loss from the £4,000 payment onwards (subject to a deduction for Mrs T'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 Mrs T may have been at risk of financial harm from fraud and the steps they should have taken before allowing the £4,000 payment to leave her account.

Should Mrs T bear any responsibility for her losses?

I've thought about whether Mrs T should bear any responsibility for her 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 Mrs T's own actions and responsibility for the losses she 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, C's platform showing Mrs T's funds used to complete the tasks. And I'm also mindful that Mrs T spoke with the scammer and customer service team at length, was added to a group chat with other 'employees' and received what R has described as comprehensive training.

I must however also take into account that, while Mrs T says she was actively looking for

work, she was offered a job opportunity on an instant messenger application from an unknown person. I also haven't seen anything to show that Mrs T received a contract of employment before starting the job with C – which I consider a legitimate employer would be expected to provide. And here, Mrs T was told she could earn daily commission of up to 200 USDT (circa £150) in addition to a salary based on the number of days worked. Given Mrs T was told that the job would take 30 – 40 mins per day, I think this is an unrealistically high return for completing relatively simplistic tasks that required a "*single click*". It would therefore have been reasonable to have expected Mrs T to have questioned whether the job opportunity was too good to be true. I'd also note that the requirement of having to pay £4,000 was significantly greater than what Mrs T was led to believe she would earn at this point too. And so, this should've been seen as excessive and suspicious.

Furthermore, I think it is reasonable for Mrs T to have questioned the legitimacy of the job opportunity given the requirement for her to purchase crypto – and a significant amount at the £4,000 point. The concept of having to falsely drive product data to gain more exposure to attract customers ought to have been seen by Mrs T as likely illegitimate. And the fact Mrs T 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 Mrs T did) as part of a job.

Because of this, and taking everything into account, I think Mrs T ought to have had sufficient reason to suspect that the job opportunity wasn't legitimate. And so, while the instant message conversation between Mrs T and the scammer shows she did have some concerns, I would've expected Mrs T to have taken greater caution before proceeding - and not simply relied on what the scammer told her. This could've included carrying out online research into this type of job online. Or Mrs T could've contacted the recruitment firms or her banking provider(s) to query whether this type of employment – and the contact she'd received - was genuine. If Mrs T had done so, then I consider she would've most likely uncovered that she was being scammed – thereby preventing her losses.

I've concluded, on balance, that it would be fair to reduce the amount Revolut pays Mrs T because of her 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 Mrs T's money?

It appears that the £1,500 transaction was refunded into Mrs T's account. But if this credit was in relation to another transaction, I don't think Revolut could've reasonably done anything to recover the £1,500 anyway. This is because the payment was to a legitimate crypto exchange and, as I understand, the funds would've then been forwarded to the scammer. This means there wouldn't have been any recoverable funds.

The debit card payments were also made to a legitimate crypto exchange. I don't consider that chargebacks had any reasonable prospect of success given there's no dispute that the crypto exchange provided crypto to Mrs T, which she subsequently sent to the scammers.

I note however that Revolut did raise chargebacks for the debit card payments. While I wouldn't have expected this, I understand that the four £190 transactions were refunded. I don't however think Revolut could reasonably have done anything more to recover the other debit card payments.

Putting things right

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

for her loss of the use of money that she might otherwise have used.

My final decision

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

- 50% of the two final payments - £3,725.
- 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 Mrs T to accept or reject my decision before 29 April 2025.

Daniel O'Dell
Ombudsman