DRN-5195399

The complaint

Miss D complains that Revolut Limited won't refund money she lost when she was the victim of a scam.

Miss D 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 June 2023 Miss D fell victim to a task-based job scam. She's explained that, at a time when she was looking for work, she was contacted on an instant messenger app offering her a remote-working job. She confirmed her interest and was contacted by a scam recruitment consultant, who explained the details of a job role available with a scam firm (that I'll refer to as 'U'). The scammer explained that the job with U involved helping merchants generate consumer data to improve product reviews and ratings. And she was told that she would receive a weekly salary plus commission for completing the 'tasks'.

Miss D received a link to U's platform for her to set up an account and she was also invited to a group chat with other agents in it. The scammer then provided instructions to Miss D on how she could complete the daily tasks. To do this, she was required to fund her account which would then be used to boost the sales of various items. Miss D went on to make the following payments to the scam via two legitimate crypto exchanges (which I'll refer to here as 'B' and 'C'):

Date (time)	Type	Payee	Amount
5 June 2023 (15:17)	Debit card	B	£1,662.59
5 June 2023 (15:27)	Debit card	B	£15
5 June 2023 (16:17)	Debit card	B	£3,505.72
5 June 2023 (19:46)	Debit card	C	£8,144.17
		Total	£13,327.48

Miss D also attempted to make a payment of about £1,500 prior to those listed above (to another crypto exchange), but this was cancelled by her during the online transfer process. And Revolut also declined a card payment to B that Mrs D attempted at 16:03 due to fraud concerns.

Miss D realised that she'd been scammed when, after consistently funding her account, her account went into a negative balance and the scammer was becoming very pushy, trying to force her to send more money – including taking out loans and borrowing from friends and family.

Miss D notified Revolut that the payments were made as part of a scam on 28 June 2023. And C complained to Revolut, on Miss D's behalf, two days later. In short, they said:

- The payments were highly unusual for Miss D's account as she hadn't invested before and was processing consecutive payments to an unusual payee(s) associated with crypto. Such activity is in line with patterns of fraud and financial crime, which is well-known across the banking sector. Each payment therefore was a missed opportunity on Revolut's part to implement an effective warning and detect the scam at the earliest opportunity.
- Had Revolut intervened and implemented effective questioning and warnings, they could've broken the spell of the scammer and stopped the scam from escalating further.
- Miss D had a reasonable basis to believe this scam was genuine. She was an inexperienced investor, and the scammer built a strong rapport with her – coming across knowledgeable and experienced in their field. Miss D searched U online, finding their website as the top result – and she says it appeared credible as it mimicked the features of a genuine website.
- Revolut failed in their duty of care to protect Miss D from the scam. And their lack of action resulted in Miss D suffering her loss.
- To settle this complaint, they said Miss D would accept a full reimbursement of her losses, 8% interest and £300 compensation.

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

- They take this type of situation very seriously as their customer's account safety is important to them. Therefore, they've implemented improved security measures to minimise and prevent the chance of such events happening.
- They referred to resources available to their users – including articles on fraud and scams. And they referenced their terms and conditions which Miss D agreed to when she created her account.
- When it comes to card payments, they recommend their client raise a chargeback – and provided directions on how to do so. But they noted that there is no guarantee their chargeback team will not reject them as the payments were authorised by Miss D. And another important element to note is that Revolut weren't involved in the fraudulent transactions directly to the scammers – as the funds were sent to legitimate crypto exchanges before being forwarded to the scammers.
- They directed Miss D to other authorities that she could report this matter to.

The complaint was referred to the Financial Ombudsman and our Investigator thought it should be upheld in part. He thought Revolut ought to have had concerns (that Miss D might be at risk of financial harm) by the point of the £3,505.72 payment. And so, Revolut should've provided a tailored written warning relevant to crypto investment scams. Had they done so, our Investigator considered Miss D would've reacted positively to it and not made any further payments.

Our Investigator thought Miss D should share responsibility for her loss. And so, he recommended Revolut refund 50% of the last two payments – along with paying 8% simple interest to Miss D for loss of use of money.

C confirmed Miss D'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 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 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.
- Gross negligence
    - Under the proposed reimbursement scheme and consistent with the CRM code, PSPs are exempted if the customer has acted with gross negligence.
    - They've shown that Revolut gave warnings which were negligently ignored by Miss D. So, Miss D continued making payments under the instructions of the scammer even though Revolut had stopped a suspicious transfer and provided her with a strong warning about scams.
    - Miss D failed to conduct due diligence and there were negative reviews about U published before the first reported payment had been made. And Miss D was promised wages of almost £5,000 per month, which is clearly too good to be true – especially coming from an unknown third party. This demonstrates the requisite degree of carelessness required to displace any liability Revolut might otherwise have had.
    - The Ombudsman upholding a complaint, in that Revolut should reimburse Miss D, without proper regard to the extensive warnings given or to the her lack of care is irrational.
- Factual considerations and findings
    - They've seen a number of decisions recently whereby the Financial Ombudsman has failed to consider relevant evidence and has reached irrational conclusions on the likely counterfactual if different warnings had been given.
    - While these are fact specific, common issues include accepting customer testimony, which is inconsistent with prior behaviour, preferring customer testimony where they have already been shown to have deliberately misled Revolut about the purpose of the transactions.
    - Respectfully, they believe that has occurred in this case by making a decision on the basis *["I don't think it's fair to find that Miss D would've ignored a tailored warning provided for the £3505.72 payment. I think had Revolut provided a tailored warning here, Miss D would've stopped this payment and any further payments made to this scam..."]* even though the customer made four further payments after receiving their targeted warning about investment scams.

Our Investigator asked Revolut for clarification on what exact warning they provided Miss D in respect of the £1,500 payment that she attempted, but cancelled, during the online transfer process.

Revolut explained the payment was temporarily put on hold, and they showed Miss D a message asking her to provide them with the purpose of the payment, which was followed by educational stories regarding the type of potential scam (based on which option was selected). But as Miss D didn't complete the stories and closed the pop-up warning, they don't know which option was selected as it isn't recorded on their system. And so, they cannot confirm what Miss D specifically saw. But the fact remains that Miss D dismissed their warning, where they informed her the transfer could be a scam, and chose to proceed – indicating that she was aware of the risks involved and was comfortable with it.

The matter was passed to me to decide. I issued a provisional decision on 22 November 2024, and I said:

> *"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 Miss D 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.

<u>Should Revolut have recognised that Miss D was at risk of financial harm from</u>

fraud?

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

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

I'm aware that crypto exchanges, like the ones Miss D made her 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 Miss D'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 Miss D 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 Miss D'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 Miss D might be at a heightened risk of fraud that merited its intervention.

While Revolut should've identified the payments were going to a crypto provider (B is a well-known crypto provider), the first two successful payments 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 third and fourth payments however, which again would've been identifiable as going to a crypto provider (B and C), were significantly greater in value than those that proceeded them and made in a very short period of time (which is a known indicator 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 Miss D 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 Miss D before these payments went ahead.

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

<u>What did Revolut do to warn Miss D</u>

Revolut has confirmed they put Miss D's transaction of about £1,500, which she attempted prior to the successful payments, temporarily on hold. They then showed Miss D a message asking her to provide the purpose of the payment, which was followed by educational stories regarding the type of scam based on the option she selected. Revolut cannot however confirm what warning Miss D saw as she didn't complete the stories and closed the pop-up warning. Miss D has said she recalls when attempting this transfer that Revolut provided a potential scam prompt about the company (which was neither B nor C). And so, she decided against obtaining crypto through that method.

Given Revolut is unable to evidence exactly what warning was provided, I can't be

sure that, if one was seen by Miss D, or that it would've been appropriately tailored to her circumstances. That being, specific to crypto scams. It follows that I can't reasonably conclude that this warning was sufficient or proportionate to the risk the last two payments – of £3,505.72 and £8,144.17 - presented. So, even if a warning of some type was presented to Miss D when she attempted to make the first payment, which she ultimately cancelled, I think Revolut needed to do more before processing the last two payments.

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 Miss D attempted to make the £3,505.72 payment, knowing (or strongly suspecting) that the payment was going to a crypto provider, to have provided a tailored warning that was specifically about the risk of crypto scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of crypto scams, without significantly losing impact.

So, at this point in time, I think that such a warning should have addressed the key risks and features of the most common crypto scams – crypto investment scams. The warning Revolut ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of common crypto investment scams, for example referring to: an 'account manager', 'broker' or 'trader' acting on their behalf; moving crypto to a third-party trading platform; the use of remote access software and a small initial deposit which quickly increases in value.

I recognise that a warning of that kind could not have covered off all scenarios. But I think it would have been a proportionate way for Revolut to minimise the risk of financial harm to Miss D by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

In relation to the final payment however, I don't consider a tailored written warning would've been a proportionate response to the identifiable risk – that being, by this point, four payments exceeding £13,000 in value in less than a four-hour period to two crypto merchants. And so, I think a proportionate response to that risk would be for Revolut to have attempted to establish the circumstances surrounding the payment before allowing it to debit Miss D's account. I think it should have done this by, for example, directing Miss D to their in-app chat to discuss the payment further.

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

I've thought carefully about whether such a warning would've resonated with Miss D for the third payment, and to the extent whereby she wouldn't have proceeded with making the payment. Having done so, I don't think it would. This is because the most common features of crypto investment scams – which, as per above, I would've expected Revolut to have highlighted – wouldn't have been relevant to Miss D's

circumstances. Miss D wasn't making the payments for investment purposes, nor had she come across the opportunity through an advertisement on social media. And while there was a third party that had guided her on how to complete the tasks as part of the job, they weren't acting on her behalf.

It follows that, while I think Revolut ought to have taken additional steps before processing this transaction, I'm not persuaded that even if Revolut had provided a tailored written crypto scam warning that it would've deterred Miss D from making the £3,505.72 payment. Because of this, I don't think Revolut's failure to provide such a warning led to Miss D suffering this part of her loss (or that which preceded it).

I do however think that, had Revolut contacted Miss D to establish the circumstances surrounding the final payment, they would've most likely prevented this loss. This is because I think it's most likely that Miss D would've been open and honest about the purpose of the payment if questioned about it. This is supported by conversations she held with her bank, in which she used to fund her Revolut account, whereby Miss D told them she was sending the funds to Revolut for crypto purposes due to the bank not 'working with that'. She also alluded to the reason for transferring the funds was due to something 'like a sort of work that requires crypto' - although Miss D wasn't questioned further about this.

Having reviewed the chat conversation between Miss D and the scammer, I also haven't seen anything to show that she was being told (or that she agreed) to mislead Revolut about the payments if questioned. Nor has Revolut provided anything to evidence Miss D would've misled them about the purpose of the payment.

So, had Revolut contacted Miss D to establish the circumstances surrounding the final payment as I would've expected, then I consider Miss D would've likely explained that she 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 Miss D had come across this job opportunity through being messaged on an instant messenger app. And that she was purchasing crypto to send to U's platform for it to be used to complete tasks, which involved using the funds to boost the sales of items.

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

<u>Is it fair and reasonable for Revolut to be held responsible for Miss D's loss?</u>

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 final payment was made to another financial business and that the payments that funded the scam were made from other accounts at regulated financial businesses. But as I've set out in some detail above, I think that Revolut still should have recognised that Miss D might have been at risk of financial harm from fraud when she made the £8,144.17 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 Miss D 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 Miss D's own account does not alter that fact and I think Revolut can fairly be held responsible for Miss D'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 Miss D 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 Miss D could instead, or in addition, have sought to complain against those firms. But Miss D has not chosen to do that and ultimately, I cannot compel her to. In these circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Miss D's compensation in circumstances where: Miss D 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 Miss D's loss from the £8,144.17 payment made on 5 June 2023 (subject to a deduction for Miss D's own contribution which I will consider below). As I have explained, the potential for multi-stage scams, particularly those involving crypto, ought to have been well known to Revolut. And as a matter of good practice and as a step to comply with its regulatory requirements, I consider Revolut should have been on the look-out for payments presenting an additional scam risk including those involving multi-stage scams.

Furthermore, I'm aware that Revolut has referenced the CRM code and the PSR's reimbursement scheme for APP scams – and their exemptions if the customer has acted with gross negligence. 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 Miss D may have been at risk of financial harm from fraud and the steps they should have taken before allowing the final payment to leave her account.

<u>Should Miss D bear any responsibility for her losses?</u>

I've thought about whether Miss D 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 Miss D'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, U's platform showing Miss D's funds and them being used to complete the tasks. I'm also mindful that Miss D spoke with the scammers at length, and they appeared to her as being highly professional and knowledgeable – thereby reassuring her about the legitimacy of the opportunity.

I must however also take into account that, while Miss D was looking for work and had signed up with recruitment agencies, she was offered a job opportunity from a recruitment agency on an instant messenger app. At which point, I should note that I've not seen any evidence to show Miss D submitted her details to the recruitment agency that contacted her (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 Miss D received any contract of employment before starting the job with U – which, similarly, I would expect to see provided by a legitimate employer. Particularly given Miss D was told that she could expect to earn about £5,000 per month – which, I would add, is an unrealistically high return for completing a relatively simplistic task of simulating the purchasing of items. It would therefore have been reasonable to have expected Miss D to have questioned whether the job opportunity was too good to be true.

Furthermore, I think it is reasonable for Miss D to have questioned the legitimacy of the job opportunity given the requirement for her to purchase significant amounts of crypto in order to simulate the purchase of items. The concept of undertaking fake purchases to boost the popularity of items ought to have been seen by Miss D as likely illegitimate. And the fact Miss D 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 Miss D did) as part of a job.

Because of this, and taking everything into account, I think Miss D ought to have had sufficient reason to suspect that the job opportunity wasn't legitimate. And so, I would've expected Miss D to have taken greater caution before proceeding. This could've included carrying out online research into this type of job online. Or Miss D could've contacted the recruitment firms she'd been in contact with to check the contact she'd received was genuine. If Miss D 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 Miss D in relation to the final payment 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 Miss D's money?

The payments were made by card to legitimate crypto exchanges. Miss D 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 exchanges provided crypto to Miss D, which she subsequently sent to the fraudsters.

…

My provisional decision

My provisional decision is that I uphold this complaint in part. I intend to direct Revolut Ltd to pay Miss D:

- *50% of the final scam payment - £4,072.09.*
- *8% simple interest, per year, on £4,072.09 calculated from 5 June 2023 to the date of settlement less any tax lawfully deductible."*

Revolut didn't respond to my provisional decision.

C confirmed Miss D's acceptance.

Given both parties have had the opportunity to respond, I can now proceed with making my final decision on this complaint.

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 the absence of any further points for my consideration, I see no reason to depart from the above. I therefore remain of the view that Revolut is responsible for the loss Miss D suffered from the point of the final payment. And that it would be fair to reduce the award by 50% due to contributary negligence on Miss D's part in these circumstances. It follows that I think Revolut should refund £4,072.09 to Miss D and pay 8% simple interest to recognise the loss of use of money she suffered.

My final decision

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

- 50% of the final scam payment - £4,072.09.
- 8% simple interest, per year, on £4,072.09 calculated from 5 June 2023 to the date of settlement less any tax lawfully deductible.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss D to accept or reject my decision before 10 January 2025.

Daniel O'Dell
Ombudsman