

## The complaint

Miss A complains that Revolut Limited ('Revolut') won't reimburse the funds she lost when she fell victim to a scam.

## What happened

Miss A says that she was abroad and needed funds so was looking at online jobs. In September 2023 she received a message from a recruitment agency asking her if her details could be passed on in respect of a potential role. Miss A agreed and received a message from a representative of a company I'll call M in this decision. Miss A didn't know at the time, but M was a clone of a genuine company and the person she was communicating with was a scammer.

The role involved completing sets of tasks to increase the visibility of products and earn commission and a salary. Miss A was advised to set up an account on M's platform to complete the tasks. She was required to maintain a positive balance on the platform, which was funded by buying cryptocurrency via a cryptocurrency exchange and transferring it to wallet address details provided by the scammer. As time went on, Miss A began to receive combination tasks which meant that she had to pay greater amounts to clear negative balances on the platform before she could complete tasks and withdraw commission.

I have set out below the payments Miss A made that related to the job scam.

Transaction	Date	Amount	Payee	Method
1	25/09/23	£12	Cryptocurrency exchange 1	Card
2	27/09/23	£49	Cryptocurrency exchange 2	Card
3	29/09/23	£4,755	Cryptocurrency exchange 2	Card
4	29/09/23	£50	Cryptocurrency exchange 2	Card
5	02/10/23	£960	Cryptocurrency exchange 2	Card
6	07/10/23	£2,500	Cryptocurrency exchange 2	Card
7	09/10/23	£2,000	Cryptocurrency exchange 2	Card
8	10/10/23	£3,000	Cryptocurrency exchange 2	Card

As Miss A had insufficient funds to clear her negative balances, she borrowed £5,000 from her mum and £1,000 from her sister. But she was told she needed to pay further amounts so looked online and provided some details to loan companies. Miss A received a message from one company, which I'll call C, asking her to call. C told Miss A that before the loan could be released, she needed to make a payment for insurance. Once she had made the payment, Miss A was asked to make further payments on the basis that previous payments hadn't been received, and because her credit rating was low. On 27 October 2023 she made faster payments relating to the loan of £150, £151, £199, £99.10, and £99.01 to a named individual (K).

When Miss A was asked to make further payments before she received the loan, she realised she had fallen victim to a scam and contacted Revolut via its chat on 27 October 2023. She later reported the job scam on 20 November 2023.

Revolut issued a final response that only covered the loan scam. Revolut said that Miss A authorised the payments and that when she set K up as a new payee it provided her with a warning. It had also done all it could to recover Miss A's funds.

Miss A was unhappy with Revolut's response and complained to this service about both scams. This service noted that Revolut hadn't provided an answer on the job scam. Revolut then considered Miss A's job scam but didn't agree to reimburse her. It said that Miss A authorised all of the payments and it had no chargeback rights.

#### *Our investigation so far*

The investigator who considered this complaint recommended that it be upheld in part. She said that Revolut was partly responsible for Miss A's loss from payment three in the table above onwards, as it should have recognised it carried an increased risk given its value and that it was clearly related to cryptocurrency. Given the risk posed, the investigator said Revolut should have asked Miss A a series of questions to narrow down the specific scam risk and provide a written warning tailored to that risk – which would have resonated with Miss A and prevented her further loss. But Miss A's actions meant she should share responsibility for her loss. Finally, Revolut had done what it could to recover Miss A's funds.

The redress recommended by the investigator was complicated by the fact another firm awarded Miss A £1,010 more than it should have in respect of the same scam. The investigator said Revolut should deduct this amount from the 50% award.

Revolut didn't agree with the investigator's findings and asked me to consider the following points:

- These are self-to-self payments, and the fraudulent activity didn't occur on Miss A's Revolut account.
- Revolut accounts are not usually used as current accounts but to facilitate payments for a specific purpose. The transactions Miss A made weren't unusual or out of character for an electronic money institution (EMI) account.
- This service's reliance on R (on the application of Portal Financial Services LLP) v FOS is misconceived.
- It is relevant to consider possible other bank intervention or warnings as funds came from Miss A's external bank account.
- It may be relevant for this service to exercise its power to inform Miss A that it may be appropriate to make a complaint against another respondent.

I intended to make a different award to the investigator, so I issued a provisional decision on 10 April 2025 which gave both parties the opportunity to respond. My provisional decision was that Revolut should reimburse 50% of all scam payments Miss A made (covering both scams), from and including the payment of £4,755 (payment three in the table above). In the 'What I've provisionally decided – and why' section of my provisional decision I said:

"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 Electronic Money Institution ("EMI") such as Revolut is expected to process payments and withdrawals that a customer

authorises it 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 the consumer modified the starting position described in *Philipp*, by 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*".

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 its contract with the consumer and the Payment Services Regulations to carry out their instructions promptly, except in the circumstances expressly set out in its contract, which included where regulatory requirements meant it 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 it could delay or refuse a payment – so far as is relevant to this complaint – to those where applicable regulations demanded that it do so, or that it make further checks before proceeding with the payment. In those cases, it 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 to 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 its 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, it 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;<sup>1</sup>
- 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 August 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through its 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

---

<sup>1</sup> For example, Revolut's website explains it launched an automated anti-fraud system in August 2018:

[https://www.revolut.com/news/revolut\\_unveils\\_new\\_fleet\\_of\\_machine\\_learning\\_technology\\_that\\_has\\_seen\\_a\\_fourfold\\_reduction\\_in\\_card\\_fraud\\_and\\_had\\_offers\\_from\\_banks/](https://www.revolut.com/news/revolut_unveils_new_fleet_of_machine_learning_technology_that_has_seen_a_fourfold_reduction_in_card_fraud_and_had_offers_from_banks/)

control its affairs responsibly and effectively, with adequate risk management systems” (FCA Principle for Businesses 3).

- Over the years, the FCA, and its 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 its customer’s accounts and scrutinise transactions.
- The October 2017, BSI Code<sup>2</sup>, 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<sup>3</sup>, 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 its products avoid causing foreseeable harm (PRIN 2A.2.10G). One example of foreseeable harm given by the FCA in its 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”*<sup>4</sup>.
- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency<sup>5</sup> when considering the scams that its 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 cryptocurrency wallet held in the consumer’s own name. And, increasingly, we have seen the use of an EMI

---

<sup>2</sup> BSI: PAS 17271: 2017” Protecting customers from financial harm as result of fraud or financial abuse”

<sup>3</sup> Prior to the Consumer Duty, FCA regulated firms were required to “pay due regard to the interests of its customers and treat them fairly.” (FCA Principle for Businesses 6). As from 31 July 2023 the Consumer Duty applies to all open products and services.

<sup>4</sup> The Consumer Duty Finalised Guidance FG 22/5 (Paragraph 5.23)

<sup>5</sup> Keeping abreast of changes in fraudulent practices and responding to these is recognised as key in the battle against financial crime: see, for example, paragraph 4.5 of the BSI Code and PRIN 2A.2.10(4)G.

(like Revolut) as an intermediate step between a high street bank account and cryptocurrency 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 it 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 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 its 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 its products, including the contractual terms, enabled it 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 cryptocurrency 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.

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

#### *Should Revolut have recognised that Miss A was at risk of financial harm from fraud?*

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

Whilst I have set out in detail in this decision the circumstances which led Miss A 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 A might be the victim of a scam.

But, when these payments were made, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency for some time. Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions.

I recognise that, as a result of the actions of other payment service providers, many customers who wish to purchase cryptocurrency 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 cryptocurrency purchases made using a Revolut account will be legitimate and not related to any kind of fraud. 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 cryptocurrency 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 A made, 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 cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

In those circumstances, as a matter of what I consider to have been fair and reasonable and good practice, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. The introduction of the FCA's Consumer Duty, on 31 July 2023, further supports this view. The Consumer Duty requires Revolut to avoid causing foreseeable harm to its customers by, among other things, having adequate systems in place to detect and prevent scams.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact most of the payments in this case were going to an account held in Miss A's own name should have led Revolut to believe there wasn't a risk of fraud.

I've gone onto consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Miss A might be at a heightened risk of fraud.

I'm satisfied that when Miss A made the £4,755 payment on 29 September 2023 Revolut should have identified that it carried a heightened risk of financial harm and should have taken additional steps before allowing it to debit Miss A's account. The payment was identifiable for cryptocurrency and was for a relatively large amount. Prior to this payment Miss A had made low value payments of below £500 (with most payments significantly below this figure) and hadn't bought cryptocurrency.

#### What did Revolut do to warn Miss A?

No warnings were provided in respect of the card payments.

Turning to the faster payments, Revolut says that when each new payee was set up it provided Miss A with the following warning:

*"Do you know and trust this payee?"*

*If you're unsure, don't pay them, as we may not be able to help you get your money back. Remember, fraudsters can impersonate others and we will never ask you to make a payment."*

This warning is very general in nature and it's difficult to see how it would resonate with Miss A.

*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.

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. It, along with other firms, has 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 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.

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 a firm should, by September 2023, on identifying a heightened scam risk, 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 it to provide more tailored warnings.

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

I am satisfied that, by September 2023 Revolut ought, fairly and reasonably, to have attempted to narrow down the potential risk further. When Miss A made payment three, Revolut should – for example by asking a series of automated questions designed to narrow down the type of cryptocurrency related scam risk associated with the payment she was making – have provided a scam warning tailored to the likely cryptocurrency related scam Miss A was at risk from.

In this case Miss A was falling victim to a job scam. As such, I'd have expected Revolut to have asked a series of simple questions to establish that this was the risk the payment presented. Once that risk had been established, it should have provided a warning which was tailored to that risk and the answers Miss A gave.

The warning Revolut ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of job scams. For example, Revolut could have explained that these scams might involve being approached via a messaging app with a part-time job/remote opportunity, 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 any money.

*If Revolut had provided a warning of the type described, would that have prevented the losses Miss A suffered from payment three onwards?*



Whilst I cannot know for certain what would have happened if Revolut had provided the warning I think it should have, I'm satisfied that it's more likely than not that the scam could've been prevented from this point onwards. I'll explain why in more detail below.

I see no reason why Miss A wouldn't have heeded a warning from Revolut, as the expert in this matter. Miss A was trying to earn some additional money because she was already in a difficult financial position, so she couldn't afford to lose these funds. When she made payment three, Miss A hadn't built a trusting relationship with the scammer and hadn't withdrawn any funds.

I have considered the chat messages Miss A exchanged with the scammer and can't see that she was provided with a cover story or told to lie to her bank. The only advice the scammer gave was that Miss A should say she was using her own cryptocurrency account – which was true – and that banks don't like cryptocurrency. On the day payment three was made, another bank asked Miss A about source of funds. Miss A said she had transferred funds to that bank account to make it easier to buy cryptocurrency. When Miss A told the scammer that this is what she said the scammer didn't make a comment or coach Miss A.

Overall, I think if Revolut had explained the main elements of a job scam, all of which applied to Miss A's circumstances, she would have realised that the job offer was not genuine and not made further payments.

*Is it fair and reasonable for Revolut to be held responsible for Miss A's loss?*

In reaching my decision about what is fair and reasonable, I have taken into account that Revolut were the intermediary in this payment journey. Miss A transferred funds from an account she held with a bank, to Revolut, then on to a cryptocurrency account held in her name.

But as I've set out in some detail above, I think that Revolut still should have recognised that Miss A might have been at risk of financial harm from fraud when she made payment three, and in those circumstances it should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it would have prevented the losses Miss A 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 Miss A's own account does not alter that fact and I think Revolut can fairly be held responsible for Miss A'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.

This service has considered complaints against other firms, as explained by the investigator in her view. Complaints have been brought by two banks and this service has sought information from another bank Miss A sent payments from that she has hasn't raised a complaint against (which didn't intervene). The redress she recommended, which I agree with, took into account her view on whether other firms have missed the opportunity to intervene or failed to act fairly and reasonably in some other way.

*Should Miss A bear any responsibility for her losses?*

In considering this point, I've taken into account what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.

Having carefully considered the circumstances, I'm satisfied that it's fair for Miss A to share responsibility for her loss with Revolut from payment three.

I recognise that there were relatively sophisticated aspects to this scam, not least a platform, which was used to access and manage the user's apparent earnings and tasks and the use of the name of a genuine company. I can imagine this would have given some validation to the scheme.

But on balance, I think a 50% deduction (from payment three) is fair and reasonable in all the circumstances of this case. The nature of the job was unusual, and I think this ought to have led Miss A to ask questions, complete some additional research and to look at reviews. Miss A was told that she would earn a significant amount of money for work that does not appear to be particularly time-consuming or arduous (\$500 for five consecutive days work, plus commission). And buying and transferring cryptocurrency to be paid is very unusual and ought reasonably to have caused concern. Miss A also didn't have a contract or any other documentation, which is unusual when taking on a new role.

Turning to the recovery scam, again Miss A wasn't provided with any terms of business, a loan agreement, or an email with C's details on. Although she wished to take out a loan she was asked to make an upfront payment. Miss A was then advised to make the payment again because it had the wrong reference. This was an unusual request, and she was able to see that her first transaction was processed. It's also clear from her chat messages with the scammer that Miss A was asked to use the paying friends and family payment reason when this wasn't accurate, and that she received a confirmation of payee no match. So I think it's fair to make a 50% deduction in respect of the recovery scam payments too.

### Recovery

As Miss A received the cryptocurrency she bought (before passing it on to the scammer) she has no chargeback rights in respect of the card payments. I'm persuaded Revolut did what it could to recover the funds Miss A transferred to K. As is often the case, funds were moved on quickly and no funds remained.

### Distress and Inconvenience

Miss A reported the job scam to Revolut on 20 November 2023. On 6 December 2023 she asked Revolut about the progress of both scam claims. Revolut gave its answer on the loan scam on 8 December but made no mention of the job scam. In her response Miss A referred to the other scam ("I'm guessing I won't get my money back from the other scam either"). The Revolut adviser ignored this and responded by saying Revolut had done everything it could. Miss A then said she'd like to complain about how both her scam cases were handled and asked for a final response.

The first time Revolut provided a response in respect of Miss A's job scam claim was on 22 August 2024 when it sent a response to this service. This was nine months after the claim was raised. Miss A was put to additional unnecessary stress and inconvenience in getting a response to her job scam claim. As a result, I'm provisionally minded to require Revolut to pay her £200 compensation.

### Provisional award

The investigator who considered this complaint said that another bank had overpaid Miss A in respect of payments made in the same scam. She recommended that this additional amount be deducted from the amount she asked Revolut to pay so that Miss A didn't receive double benefit. But the payments Miss A made from that bank went directly to her cryptocurrency account and didn't pass through Miss A's Revolut account. So they aren't relevant to this complaint. I'm not persuaded that because another bank paid more than this service would award on a goodwill basis the additional amount should be deducted from my award against Revolut.

Miss A credited her Revolut account with funds from two different bank accounts to the one I have discussed above. One of these banks hasn't been held responsible for any of the transfers to Revolut, and there is no complaint about the other. So I am provisionally requiring Revolut to reimburse 50% of all transactions from and including payment three (including all transactions to K, as if Revolut had done what I think it should have, these payments wouldn't have been made)."

### Responses to my provisional decision

Miss A let me know that she agreed with my provisional decision. Revolut didn't respond by the deadline set.

Under the Dispute Resolution Rules (found in the Financial Conduct Authority's Handbook), DISP 3.5.13, says if a respondent (in this case Revolut) fails to comply with a time limit, the ombudsman may proceed with the consideration of the complaint. So I am issuing my final decision.

### **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.

As neither party has raised any new points or asked me to consider any new evidence my decision is the same as my provisional decision, and for the same reasons (which I have set out in full above).

In summary, I think Revolut should have recognised that payment three in the table above carried an increased risk of harm and taken steps to narrow down the likely scam risk by, for example, asking a series of automated questions. Once it had narrowed down the scam risk Revolut should have provided a tailored written warning. As Miss A was falling victim to a job scam (at this point) Revolut should have provided a warning that covered the essential elements of a job scam. Had it done so, I consider Miss A's further loss would have been prevented and she would not have fallen victim to the loan scam.

On balance though, I consider it fair and reasonable for Miss A to share responsibility for her loss with Revolut from payment three onwards. There were some concerning features about both scams that ought reasonably to have led Miss A to complete some checks. I will mention a few here. The nature of the job with M was unusual and Miss A was told she could earn a significant amount for completing simple tasks. There was no contract and being asked to buy cryptocurrency to be paid is very unusual. Turning to the loan scam, Miss A again wasn't provided with any documents. She was also asked to pay upfront fees to an individual rather than a company and to provide an incorrect payment reason.

I'm also persuaded that Revolut should pay Miss A £200 compensation for the additional stress and inconvenience its poor service caused. Revolut didn't give Miss A an answer in respect of her job scam claim for nine months.

The investigator recommended that a deduction be made from the amount Revolut paid Miss A because another bank made a goodwill payment that was higher than she would recommend. But the payments from the other bank weren't passed through Miss A's Revolut account – they went straight to a cryptocurrency provider. In the circumstances, they have no relevance to this complaint.

Overall, I consider Revolut should reimburse 50% of all scam payments from payment three in the table above (including the loan scam payments).

### **My final decision**

I uphold this complaint and require Revolut Ltd to:

- Reimburse Miss A 50% of all transactions from and including payment three - £6,981.56; and
- Pay interest on the above amount at the rate of 8% simple per year from the date of each transaction to the date of settlement; and
- Pay compensation of £200.

If Revolut Ltd is legally required to deduct tax from the interest it should send Miss A a tax deduction certificate so she can claim it back from HMRC if appropriate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss A to accept or reject my decision before 27 May 2025.

Jay Hadfield  
**Ombudsman**