

## The complaint

Mr C complains that Revolut Ltd ('Revolut') won't reimburse the money he lost to a scam.

## What happened

Mr C's complaint has been brought by a professional representative but as the account was in his name, I'll refer to Mr C throughout my decision.

### *What Mr C says*

Mr C says that he was looking for a job and had made online applications. He received a call from someone who said they received his details from a recruitment company. The caller offered him a role where he could work from home with a company I'll refer to as B in this decision. The role involved completing sets of tasks to boost the rating and ranking of applications on various app stores.

Mr C was given a trainer who helped him to set up an account on B's platform. He was required to maintain a balance on the platform, which was funded by buying cryptocurrency via an exchange I'll refer to as O and transferring it to wallet details provided to him. As time went on the tasks became more expensive, and Mr C was required to pay more to clear his negative balance before he could receive further tasks. Mr C was also asked to make payments to receive bonuses.

Mr C was told he would be paid £1,000 after successfully completing tasks on five consecutive days and that all funds used to clear his negative balance would be refunded to him.

I have set out in the table below the payments Mr C made to O.

Transaction	Date	Type of payment	Amount
1	20/09/23	Card	£17
2	21/09/23	Card	£15
3	21/09/23	Card	£10
4	21/09/23	Card	£50
5	24/09/23	Card	£390
6	24/09/23	Card	£114
7	24/09/23	Card	£25
8	25/09/23	Card	£1,150
9	25/09/23	Card	£2,750
10	25/09/23	Card	£600
11	25/09/23	Card	£1,000
12	25/09/23	Card	£1,000

13	25/09/23	Card	£1,000
14	25/09/23	Card	£1,000
<b>Total</b>			<b>£9,121</b>

After making these payments, Mr C was told he needed to pay a further amount of around £8,000 and realised he was the victim of a scam. Mr C raised a complaint with Revolut through his representative in October 2023.

#### *What Revolut says*

Revolut didn't agree to reimburse Mr C. It said that the payments were made by card but as Mr C paid O and got the cryptocurrency he paid for it had no chargeback rights. Revolut also noted that Mr C hadn't contacted it directly, so it hadn't had the opportunity to investigate his concerns.

When the complaint was brought to this service, Revolut raised the following points:

- This service is permitted to depart from the law but where we do should explain that we have done so and explain why. If we apply the law or legal duties, we should apply it correctly and if we err in law, we are susceptible to judicial review on the grounds of error in law in relation to our identification of what the law is (as well as perversity and irrationality).
- Revolut is bound by contract, applicable regulations and common law to execute valid payment instructions. The duty is strict and there are only limited exceptions. Revolut referred to specific terms in its terms and conditions and went on to say that although the relationship between a payment service provider (like Revolut) and a customer is one of contract, such contracts are performed in a heavily regulated legal environment. The most significant legislation is the Payment Services Regulations 2017 which impose obligations to execute authorised payments promptly. By suggesting that it needs to reimburse customers, it says our service is erring in law.
- This service has overstated Revolut's obligations. Revolut recognises its obligations and has put adequate procedures in place. But the duty is not absolute and doesn't require Revolut to detect and prevent all fraud.
- It does not need to concern itself with the wisdom or potential for financial loss of a customer's payment instructions. This was confirmed in the recent Supreme Court judgement in the case of *Philipp v Barclays Bank UK plc [2023] UKSC 25*.
- Our service appears to be treating Revolut as if it were a signatory to the Contingent Reimbursement Model Code.
- The Payment Service Regulator's ("PSR") future mandatory reimbursement scheme will not require it to refund payments made in these circumstances either.
- 'Self-to-self' payments don't meet either the Dispute Resolution Rules ("DISP Rules") or CRM Code definition of an APP scam.
- It is irrational and illogical for this service to hold Revolut responsible for losses when it is an intermediate link and other financial institutions in the payment chain have comparatively greater data than Revolut.

#### *Our investigation so far*

The investigator who considered this complaint didn't recommend that it be upheld. He said that Revolut drew Mr C's attention to potential scams, but Mr C chose to proceed.

Mr H didn't agree with the investigator's findings, so his complaint was passed to me to decide. In summary, he said:

- The transactions were out of character and Revolut should have intervened. On 25 September 2023 alone Mr H sent multiple payments to a known cryptocurrency exchange in quick succession. He had not used the account regularly and hadn't bought cryptocurrency for over two years. So Mr H said Revolut should have questioned him and not given an online warning.
- Had Revolut have intervened the scam would have been exposed as there were numerous red flags.
- Electronic Money Institutions like Revolut have the same regulatory requirements to prevent fraud as banks. All are expected to use fraud trends knowledge to meet good industry practice expectations.

I intended to reach a different outcome to the investigator so issued a provisional decision on 25 September 2024 so that each party had the opportunity to comment. 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 Mr C 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*".

So Revolut was required by the implied terms of its contract with Mr C 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 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 September 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 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).

---

<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/)

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

- 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 (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;

---

<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.

- 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.

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

It isn't in dispute that Mr C has fallen victim to a cruel scam here, nor that he authorised the payments he made by transfers to his cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

I'm aware that cryptocurrency exchanges generally stipulate that the card used to purchase cryptocurrency 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. So Revolut likely thought the transactions I have set out in the table above would be credited to a cryptocurrency account in Mr C's own name.

But by September 2023, 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.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mr C made in September 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 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. And, as I've set out, 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 Mr C' own name should have led Revolut to believe there wasn't a risk of fraud.

I also can't agree with Revolut that the transactions to O were in line with Mr C's stated account opening purpose of spending abroad and overseas transfers.

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 Mr H might be at a heightened risk of fraud.

I think Revolut should have identified all payments were going to a cryptocurrency provider. But transactions one to eight were low in value and in line with previous account activity, so I don't think Revolut should reasonably have suspected that they might be part of a scam. Many Revolut customers use their accounts to buy cryptocurrency legitimately and Revolut needs to strike a balance between protecting its customers and minimising disruption to legitimate payment journeys.

Payment nine was the highest value payment for six months and was the second transaction to a cryptocurrency provider in just over an hour and a half. There was an overall pattern of increasing payments which were clearly related to cryptocurrency. Given the combination of factors I consider Revolut should have considered that Mr C could be at heightened risk of financial harm from fraud and, in line with good industry practice, provided a warning before the payment went ahead.

Overall, I'm satisfied that Revolut should have identified that payment nine carried a heightened risk of financial harm and should have taken additional steps before allowing it to debit Mr H's account.

#### What did Revolut do to warn Mr C?

When Mr C set up O as a new payee Revolut provided a warning that said,

*"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 Mr C. I don't think that providing the warning above in relation to an earlier payment was a proportionate or sufficiently specific response to the risk that payment nine presented so Revolut needed to do more.

I can see that a payment on 25 September 2023 was blocked and discussed in Revolut's in app chat. Revolut hasn't said which payment the chat related to, but it appears to be in respect of a payment that came after payment nine. I say this because Revolut's transaction history shows declined payments between payments ten and eleven, and after the transactions I have listed in the table above. It would be helpful if Revolut could clarify which transaction this warning related to when it responds to this provisional decision.

The warning that was provided says payments to the merchant might not be completed and goes on to say,

*"However, we'd like to warn you that there's been an increase in scams targeting crypto investors where customers move their funds to wallets they don't control. Fraudsters show*



*victims fake investment gains, but the scam only materialises when you attempt to withdraw your funds.”*

Even if this warning was given in respect of payment nine, I'm not satisfied it went far enough or was specific enough, given that it relates to investment, and what I say below.

*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. 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 by September 2023, when these payments took place, Revolut should have had systems in place to identify, as far as possible, the actual scam that might be taking place and to provide tailored effective warnings relevant to that scam for both APP and card payments. As I explained earlier in this decision, I understand Revolut did have systems in place to identify scam risks associated with card payments which enabled it to ask some additional questions and/or provide a warning before allowing a consumer to make a card payment. I also understand in relation to Faster Payments it already had systems in place that enabled it 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 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 nine 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.

Taking that into account, I am satisfied that, by September 2023, Revolut ought, fairly and reasonably, to have attempted to narrow down the potential risk further. I'm satisfied that when Mr C made payment nine, 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 Mr C was at risk from.

In this case, Mr C was falling victim to a 'job scam' – he 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, it should have provided a warning which was tailored to that risk and the answers Mr C 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 S wouldn't have done so here.

And in the circumstances of this case, I think Revolut ought fairly and reasonably to have delayed payment nine to make further enquiries with a view to providing a specific scam warning, of the type I've described.

*If Revolut had provided a warning of the type described, would that have prevented the losses Mr C suffered from payment nine?*

I think that a warning of the type I've described would have identified that Mr C's circumstances matched an increasingly common type of scam.

I've read the messages between Mr C and the fraudsters. It's clear that by the time Mr C made the ninth payment he'd been asked to make numerous payments clear negative balances and to receive bonuses. The day before, on 24 September Mr C had expressed concern about finding additional funds and on the day of the ninth payment Mr C said it was getting out of whack. I think the messages show that Mr C was starting to have concerns about what he was being asked to do and that a warning tailored to a task based job scam would have resonated with him and made him and reinforced developing concerns.

Ultimately, I don't consider Mr C would have gone ahead with the payment if Revolut had provided a warning tailored to job scams.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr C purchased cryptocurrency which credited an e-wallet held in his own name, rather than making a payment directly to the fraudsters. So, he remained in control of his money after he made the payments from his Revolut account, and it took further steps before the money was lost to the fraudsters.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr C might have been at risk of financial harm from fraud when he made payment nine, 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 Mr C suffered. The fact that the money used to fund the scam came from elsewhere and wasn't lost at the point it was transferred to Mr C's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr C 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.

Mr C brought a complaint against another firm. This service said that firm didn't miss an opportunity to intervene and acted reasonably when Mr C transferred funds to his Revolut account. So that case doesn't impact my decision against Revolut. In this case it is appropriate to hold Revolut responsible as it could have prevented Mr C's loss. 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.

Revolut has argued in submissions to our service that we are applying the provisions of the CRM Code to complaints against it, despite it not being a signatory and in circumstances where the CRM Code would not, in any case, apply. It also argues that the Payment Service Regulator's ("PSR") proposed mandatory reimbursement scheme will not require Revolut to reimburse Mr C.

I do not seek to treat Revolut as if it were a signatory to the CRM Code. I've explained in some detail the basis on which I think, fairly and reasonably, Revolut ought to have identified that Mr C was at risk of financial harm from fraud and taken further steps before payment nine debited his account.

I'm also aware that the Payment Service Regulator's ("PSR") proposed mandatory reimbursement scheme would not require Revolut to reimburse Mr C.

The PSR's proposals are not yet in force and are not relevant to my decision about what is fair and reasonable in this complaint. But I do not consider the fact that the PSR does not propose to make it compulsory for payment service providers to reimburse consumers who transfer money to an account in their own name as part of a multi-stage fraud, means that Revolut should not compensate Mr C in circumstances when it failed to act fairly and reasonably, as I have found was the case here. Indeed, the PSR has recently reminded firms that fraud victims have a right to make complaints and refer them to the Financial Ombudsman Service that exists separately from the intended reimbursement rights and that APP scam victims will still be able to bring complaints where they believe that the conduct of a firm has caused their loss (in addition to any claim under the reimbursement rules).

I do not consider it to be relevant that the circumstances here do not fall under the specific definition of an APP scam set out in the CRM Code and DISP rules. Those definitions define the scope of the CRM Code and eligibility of payers to complain about a payee's PSP respectively. They do not preclude me from considering whether Revolut failed to act fairly and reasonably when it made payment nine without asking Mr C questions to understand the reason for the payment or providing any warnings. So, I'm satisfied Revolut should fairly and reasonably have made further enquiries before processing any further payments. If it had, it is more likely than not that the scam would have been exposed and Mr C would not have lost any more money. In those circumstances I am satisfied it is fair to hold Revolut responsible for some of Mr C's loss.

For the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Mr C's loss from payment nine (subject to a deduction for consumer's own contribution which I will consider below).

**Should Mr C bear any responsibility for his 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.

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. I note that Mr C also had access to a customer support team. I can imagine these features would have given some validation to the scheme.

But on balance, I consider a 50% deduction is fair and reasonable in all the circumstances of this case. The nature of the job was unusual and implausible, and I think this ought to have led Mr C to ask questions, complete some additional research and to look at reviews. Mr C was told that if he completed tasks on five consecutive days, he would earn £1,000. This is a significant amount for work that does not appear to be particularly time-consuming or arduous. And buying and transferring cryptocurrency to be paid is very unusual.

I also consider that at the point at which I have said Revolut needed to do more Mr C had concerns about the legitimacy of the scheme and his ability to make payments. He had been asked to pay additional sums in respect of bonuses he had not received. The scammer also offered to help Mr C and loan him money, which I consider should have concerned Mr C.

Overall, I consider it fair to reduce the amount Revolut pays Mr C to reflect the role he played in what happened.

#### *Responses to my provisional decision*

Mr C let me know that he accepts my provisional decision. Revolut didn't respond.

#### **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 for me to consider my final decision is the same as my provisional decision. I have set out my full reasoning above, so won't repeat it here.

#### **My final decision**

I uphold this complaint and require Revolut Ltd to:

- Pay Mr C £3,675; 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.

If Revolut Ltd considers that it is required by HM Revenue & Customs to deduct income tax from that interest, it should tell Mr C how much it has taken off. It should also give Mr C a tax deduction certificate if he asks for one, so he can reclaim the tax from HM Revenue & Customs if appropriate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 14 November 2024.

Jay Hadfield  
**Ombudsman**