

The complaint

Mr C complains that Revolut Ltd hasn't refunded him after he fell victim to a scam.

What happened

I issued a provisional decision for this complaint on 29 October 2024. In it I set out the background and my proposed findings. I've included a copy of the provisional decisions at the end of this final decision, in *italics*. I won't then repeat all of what was said here.

Both parties have now had an opportunity to respond to the provisional decision. Mr C accepted the outcome. Revolut didn't respond. As the deadline for responses has now expired, I'm going on to issue 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.

Having done so, I'm upholding the complaint in line with my provisional findings.

As Mr C accepted those findings, and Revolut didn't respond, there is no further evidence or argument for me to consider. I see no reason to depart from the findings and reasoning I've already explained.

Putting things right

On Mr C's confirmation of his acceptance of this final decision, Revolut should:

- refund 50% of Mr C's loss from the £3,150 payment onwards (£4,085); *and*
- pay interest on that sum at 8% simple per year, calculated from the date of loss to the date of settlement

My final decision

I uphold this complaint against Revolut Ltd.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 10 December 2024.

Provisional decision

I've considered the relevant information about this complaint.

Having done so, I'm reaching a different outcome to that recommended by our investigator.

I'll look at any more comments and evidence that I get by 12 November 2024. But unless the

information changes my mind, my final decision is likely to be along the following lines.

The complaint

Mr C complains that Revolut Ltd hasn't refunded him after he fell victim to a scam.

What happened

In February 2023 Mr C was contacted by someone he didn't know on WhatsApp. The person claimed to have obtained Mr C's details from a recruitment agent and asked if he was looking for work. Mr C didn't realise at the time, but he'd been contacted by a scammer.

Mr C was looking for a way to supplement his income and so listened to what the scammer had to say. It was explained to him that he could complete tasks in a role as a 'data promotion agent'. He was told he'd earn commission of each task that he completed. Mr C was interested and signed up.

He was directed to create a profile on a scam website and was told he'd need a cryptocurrency wallet. This was to be used to fund his employment wallet, so that he in turn could receive his commission.

Mr C started to complete the tasks and was then being told he had to credit more and more to his employment account. He made card payments from his Revolut account to a cryptocurrency wallet in his name, before sending the funds on at the scammer's instruction.

Between 12 and 27 February 2023 Mr C had made a total of 17 payments, with a total value of £8,927. The seventeenth payment was for £3,150. There were more payments that followed, with a further £5,020 sent across 11 payments over several weeks.

Mr C realised he'd been scammed when the requests for payment kept coming and he was never able to withdraw anything from the employment account. He reported what had happened to Revolut.

Revolut's response was to suggest attempting a chargeback. The transactions were raised as a dispute but successfully defended by the merchant as Mr C had made the payments.

Revolut said it wouldn't provide a refund for any other reason, stating the transactions had been properly authorised with genuine merchants and that the account activity hadn't appeared unusual or suspicious.

Mr C brought his complaint to our service as he was unhappy with Revolut's response. One of our investigator's considered the complaint and didn't recommend it be upheld. In summary, she did feel that the £3,150 payment on 27 February 2023 ought to have been met with a written scam warning. But she didn't believe it would have made a difference, as it was more likely than not Mr C would have been presented with a cryptocurrency investment scam warning, which wouldn't have had an impact on Mr C given the type of scam he was actually caught up in.

Mr C disagreed and felt Revolut ought to have deployed a human intervention. As our investigator disagreed the complaint has been passed to me for review.

What I've provisionally 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.

Having done so, I intend to uphold it. Unless I receive persuasive new evidence or arguments from either party by 12 November 2024, my final decision will be along the following lines.

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 – 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 its 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 its 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 it suspected its 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 February 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;¹*
- 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 February 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)².*
- 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*

¹ 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/

² Since 31 July 2023 under the FCA's new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.

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 Code³, 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 cryptocurrency 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 February 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;*
- 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*

³ BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

- 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 February 2023, Revolut should in any event have taken these steps.

Should Revolut have recognised that consumer 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 third parties and to his 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 Mr C to make the payments using his Revolut account and the process by which that money ultimately fell into the hands of the fraudster, I am mindful that, at that time, Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Mr C might be the victim of a scam.

Firstly, I don't think that Revolut would have had any reason to intervene in the earlier payments made toward the scam, that being payments up to just before the £3,150 was made on 27 February 2023.

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. Revolut would likely have been aware of this fact too. So, it could have reasonably assumed that those early payments would be credited to a cryptocurrency wallet held in Mr C's name.

By February 2023, when these transactions took place, 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.

By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions. And by February 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 cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

I recognise that, as a result of the actions of other payment service providers, 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 (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 cryptocurrency provider, a fact that Revolut is aware of.

So, taking into account all the above I am satisfied that by the end of 2022, prior to the payments Mr C made in February 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.

To be clear, I'm not suggesting as Revolut argues 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 cryptocurrency in February 2023 that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency 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 it processed such payments. And as I have explained Revolut was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks.

Taking all 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'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, it ought to have identified that Mr C might be at a heightened risk of fraud that merited its intervention.

I think Revolut should have identified that all payments were going to a cryptocurrency provider (the merchant is a well-known cryptocurrency platform), but those before the £3,150 are relatively low in value (I include in that description the highest value paid during that time, which was £1,340), and I don't think Revolut should reasonably have suspected that they might be part of a scam.

The payment of £3,150 was clearly going to a cryptocurrency provider. It was significantly larger than any other payment that had debited Mr C's account in the previous six months and was the seventeenth payment to a cryptocurrency provider in just 15 days.

Given what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Mr C was at heightened risk of financial harm from fraud.

In line with good industry practice, I am satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this payment went ahead.

To be clear, I do not suggest that Revolut should provide a warning for every payment made to cryptocurrency. Instead, as I've explained, I think it was a combination of the

characteristics of this payment (combined with those which came before it, and the fact the payment went to a cryptocurrency provider) which ought to have prompted a warning.

Revolut argues that it is unlike high street banks in that it provides cryptocurrency services in addition to its electronic money services. It says that asking it to 'throttle' or apply significant friction to cryptocurrency transactions made through third-party cryptocurrency platforms might amount to anti-competitive behaviour by restricting the choice of its customers to use competitors. As I have explained, I do not suggest that Revolut should apply significant friction to every payment its customers make to cryptocurrency providers. However, for the reasons I've set out above I'm satisfied that by February 2023 Revolut should have recognised at a general level that its customers could be at increased risk of fraud when using its services to purchase cryptocurrency and, therefore, it should have taken appropriate measures to counter that risk to help protect its customers from financial harm from fraud. Such proportionate measures would not ultimately prevent consumers from making payments for legitimate purposes.

There is a further layer to add to my findings on why Revolut ought to have recognised Mr C might be at risk of financial harm from fraud. And this relates to what Revolut knew about Mr C as a customer.

Revolut knew Mr C had fallen victim to two cryptocurrency related scams just months before this one: an investment scam and then a linked recovery scam. Mr C had raised scam claims with Revolut, and it had considered the outcomes of those claims. So it knew that Mr C might be, at least to some extent, vulnerable to such scams. This information ought to have been taken into account when assessing the risk posed to Mr C. And, given what I've said about what Revolut knew about the nature of the payments, and the scams landscape, the case for saying it ought to have been concerned about the payments he was making in February 2023 becomes even stronger.

What did Revolut do to warn consumer?

Revolut hasn't suggested it gave Mr C any warnings about proceeding and I've seen no evidence of it doing so.

What kind of warning should Revolut have provided?

Our investigator felt an appropriate warning from Revolut would have been a written one, setting out some key details of cryptocurrency scams. But, given what I've said above, I don't agree that would have been a proportionate response to the identifiable risk.

Having thought carefully about the risk the payment of £3,150 presented, considering what Revolut knew about the payment and Mr C, 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 Mr C's account. I think it should have done this by, for example, directing Mr C to its in-app chat to discuss the payment further.

If Revolut had provided a warning of the type described, would that have prevented the losses consumer suffered from the £3,150 payment onward?

It's evident from Mr C's actions that he was caught up in the scam and believed what the scammer was telling him. But I've seen no evidence to suggest he wouldn't have reacted positively to appropriate and proportionate engagement from Revolut. There's nothing to suggest he wouldn't have engaged with them and listened to what they had to say about what he was doing.

If asked, I believe Mr C would have revealed some very concerning features about what he was doing. I'm mindful here that this type of job scam wasn't as prevalent in early 2023 as perhaps it now is. But, even if Revolut had been completely unaware of the scam type (which I consider to be unlikely), I'm satisfied it ought fairly and reasonably to have been able to identify some very troubling features. These include but are not limited to: Mr C being contacted out of the blue by an unknown party who had not really been verified, that Mr C was being told to pay money somewhere else in order to earn wages, and that those payments were to be made in cryptocurrency.

Revolut ought then to have been able to give very strong warnings to Mr C about proceeding and to explain why it was likely he was caught up in a scam. Given his previous experiences and losses, I'm satisfied he would more likely than not have taken such warnings seriously and stopped what he was doing.

Is it fair and reasonable for Revolut to be held responsible for consumer'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.

I have carefully considered Revolut's view that in a multi-stage fraud, a complaint should be properly considered only against either the firm that is a) the 'point of loss' – the last point at which the money (or cryptocurrency) remains under the victim's control; or b) the origin of the funds – that is the account in which the funds were prior to the scam commencing. It says it is (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.

In reaching my decision, I have taken into account that the payments were made to another financial business (a cryptocurrency exchange) 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 Mr C might have been at risk of financial harm from fraud when he made the £3,150 payment, 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/or 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 consumer's loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

I've also considered that Mr C 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 consumer could instead, or in addition, have sought to complain against those firms. But Mr C has not chosen to do that and ultimately, I cannot compel them to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mr C's compensation in circumstances where: he has only complained about one respondent from which they are entitled to recover their losses in full; has not complained against the other firm (and so is unlikely to recover any amounts apportioned to that firm); and where it is appropriate to hold a business such as Revolut responsible (that could have prevented the loss and is responsible for failing to do

so). That isn't, to my mind, wrong in law or irrational but reflects the facts of the case and my view of the fair and reasonable position.

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be referred to me) and for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Mr C's loss from the £3,150 payment (subject to a deduction for his own contribution which I will consider below).

Should Mr C bear any responsibility for his losses?

I've thought about whether Mr C should bear any responsibility for his loss, from the point of the £3,150 payment. 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 the circumstances of this complaint including taking into account Mr C's own actions and responsibility for the losses he has suffered.

I recognise that there were relatively sophisticated aspects to this scam, not least an apparently credible and professional looking website, which was used to access and manage the user's apparent earnings and tasks.

But, at its heart, the scam appears to have had some features that made its plausibility questionable (though not completely so). While I haven't seen and heard everything that Mr C saw, the fraudster's explanation for how the scheme worked is difficult to understand in parts, and I think that on some level Mr C ought reasonably to have questioned whether the activity he was tasked with carrying out (which does not appear to be unduly time-consuming or arduous) was capable of generating the returns promised at the point at which he was required to make a further substantial payment.

It's also true that Mr C was contacted out of the blue by an unknown party. He didn't know who this person was and didn't really have any way of verifying who they were. Mr C has said he checked that the company the scammer said they worked for existed and found a website. But there doesn't appear to have been much done beyond that. To then go on to quickly send thousands of pounds to an unknown recipient does not seem reasonable to me.

In making these findings, I am also mindful that Mr C had been scammed before. Those scams were slightly different in nature, in that they involved investment and the recovery of lost funds. But they also both involved paying money away through cryptocurrency wallets. And Mr C ought to have been reasonably aware that such payments were untraceable and unrecoverable. He also ought fairly and reasonably to have been very cautious about receiving unsolicited contact with the promise of financial gain.

And so, with these points in mind, I find it would be fair and reasonable for Mr C to share responsibility for his loss from the £3,150 payment onwards.

Putting things right

Subject to any further evidence or arguments made that might alter my findings, and should Mr C ultimately accept, Revolut should:

- refund 50% of Mr C's loss from the £3,150 payment onwards (£4,085); and
- pay interest on that sum at 8% simple per year, calculated from the date of loss to the date of settlement.

My provisional decision

I intend to uphold this complaint against Revolut Ltd.

Ben Murray
Ombudsman