

## The complaint

Mr A is unhappy that Revolut Ltd (Revolut) won't refund the money he lost to a third-party scam.

## What happened

Mr A told us he saw a post on social media from someone he knew - promoting an investment opportunity – but unbeknown to him at the time their account had been hacked. Having registered interest in the opportunity, Mr A was then contacted by someone who said they were an accounts manager for a crypto-mining investment company (I will refer to as W).

Mr A says he was told that he would receive £6,400 on every £1,000 he invested – so he started making deposits. Mr A transferred money to a genuine payment platform (I will refer to as S) and from there he purchased cryptocurrency which was then sent to the scammer via a wallet. Mr A says he had access to an online portal and could see the investment returns he was making. But when he tried to withdraw his money, W kept giving him of different reasons as to why his withdrawal had been unsuccessful. He then realised he had been scammed and contacted Revolut. Mr A made the following payments as a result of the scam:

Payment #	Date	Payee	Amount
1	27/03/2023	S	£2,450
2	29/03/2023	S	£7,000
3	29/03/2023	S	£4,070
4	30/03/2023	S	£3,600
5	05/04/2023	S	£1,600
6	09/04/2023	S	£5,000
7	10/04/2023	S	£800
8	13/04/2023	S	£2,000
9	14/04/2023	S	£1,300
10	17/04/2023	S	£3,000
11	20/04/2023	S	£2,300
12	20/04/2023	S	£1,250
13	22/04/2023	S	£1,120
14	25/04/2023	S	£1,020
15	25/04/2023	S	£300
16	26/04/2023	S	£2,310
17	26/04/2023	S	£520
18	27/04/2023	S	£520
		Total	<b>£40,160</b>

Mr A had also made four smaller payments to S in May 2022. These were not subject to a scam or connected with the disputed transactions above.

Revolut did not refund Mr A. It said:

- All transfers were initiated and authorised by Mr A.
- The fraudulent activity did not take place on Revolut's platform. Revolut was used as an intermediary to receive funds from Mr A's main bank account that he would then transfer on to his legitimate external accounts held with S. It should not be required to refund 'self-to-self' transactions, where it is only an intermediate link in a chain of transactions.
- It gave proportionate and appropriate scam warnings.
- The scam was not a 'heat of the moment' single payment or 'out of character' transaction but an investment scam where eighteen transfers were sent over a period of thirty-one days.

Our investigator upheld the complaint in part. She felt that Revolut should have recognised that Mr A could be at heightened risk of financial harm from fraud when he made the £4,070 payment (payment three). She considered Revolut should have intervened and made further enquiries about the purpose of the payment before processing it she also felt Mr. A should share in responsibility for his losses and so recommended Revolut refund 50% of the losses from payment three.

Revolut did not accept the investigator's view. I've read all of its submission but in summary it said:

The fact that the funds were moved from another account prior to making the payments is not only normal for a Revolut and does not raise any suspicions, but it is also necessary.

The payment went to the Customer's account held within a cryptocurrency exchange service. This does not represent a red flag in any way, also considering that the majority of the payments were performed in different day and did not follow a suspicious pattern.

The balance after the mentioned transaction was £4,183 and therefore did not clear the balance and could not be considered suspicious.

Mr A performed the first payment to their account held within S in May 2022. Mr A performed further payments from March 2023 to the same beneficiary. No issues were reported since May 2022, so Revolut had no reason to consider the transactions as suspicious.

The ombudsman service is empowered to compel disclosures from either the relevant banks or from the customer themselves under the provisions of DISP 3.5.11, and specifically empowered to consider evidence from third parties under DISP 3.5.12 (which would include other financial institutions involved in multi-stage frauds). It may also be applicable for the for the ombudsman service to exercise its power under DISP 3.5.2 to inform the customer that it could be appropriate to make a complaint against another respondent.

Mr A ignored, not only the red flags during the period when the transactions were carried out, but ignored other aspects, such as the promise of a 650% profit.

If the ombudsman service departs from the law this must be acknowledged and explained.

Revolut does not owe a duty to prevent fraud or scams. It is bound by contract to execute payment instructions, and this is subject to only very limited exceptions.

Revolut recognises its obligations to put in place adequate procedures to counter the risk that it may be used to further financial crime (and has such systems and controls in place), but that duty is not absolute and does not go as far as to require Revolut to detect and prevent all fraud, particularly in the face of authorised customer instructions.

The duty to execute valid (or “authorised”) payment instructions does not require it to assess the commercial wisdom or potential for financial loss of a proposed transaction. This point was very recently recognised in the Supreme Court’s judgment in *Philipp v Barclays Bank UK plc* [2023] UKSC 25.

It appears that reimbursement has been awarded in these cases as if the voluntary Contingent Reimbursement Model code (the “Code”) or the mandatory reimbursement rules proposed by the PSR in PS23/3 applied. But Revolut is not a signatory to the Code and therefore its rules do not apply.

In a “self to self” scenario, there is no APP fraud as the payments are not passing from “person A” to any other person. The payments are leaving Revolut to an account held by and accessed by the customer at another financial institution. “Self to self” transfers also do not meet the definition of APP fraud in the Code.

It is irrational (and illogical) to hold Revolut liable for customer losses in circumstances where Revolut is merely an intermediate link, and there are typically other authorised banks and other financial institutions in the payment chain that have comparatively greater data on the customer than Revolut, but which the FOS has not held responsible in the same way as Revolut.

I issued my provisional decision on 26 September 2024. Mr A accepted my provisional decision. Revolut did not 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.

Revolut did not respond to my provisional decision.

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.

As the deadline for responses to my provisional decision has expired, I’m going to proceed with issuing my final decision. However, I think it’s unlikely that Revolut would’ve provided any new evidence or information that would’ve changed the outcome of the case.

As neither party has provided any further evidence or arguments for consideration, I see no reason to depart from the conclusions set out in my provisional decision. For completeness, I have set this out below.

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 A 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 A and the Payment Services Regulations to carry out their instructions promptly, except in the circumstances set out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

Whether or not Revolut was required to refuse or delay a payment for one of the reasons set out in its contract, the basic implied requirement to carry out an instruction promptly did not in any event mean Revolut was required to carry out the payments immediately<sup>1</sup>. Revolut could comply with the requirement to carry out payments promptly while still giving fraud warnings, or making further enquiries, prior to making the payment.

---

<sup>1</sup> The Payment Services Regulation 2017 Reg. 86 states that "the payer's payment service provider must ensure that the amount of the payment transaction is credited to the payee's payment service provider's account **by the end of the business day following the time of receipt of the payment order**" (emphasis added).

And, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Revolut should in March 2023 fairly and reasonably 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 (irrespective of whether it was also required by the express terms of its contract to do so).

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>2</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.

In reaching my conclusions about what Revolut ought fairly and reasonably to have done, 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>3</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

---

<sup>2</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/>

<sup>3</sup> BSI: PAS 17271: 2017” Protecting customers from financial harm as result of fraud or financial abuse”

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.

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 March 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
- 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.

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

It isn't in dispute that Mr A has fallen victim to a cruel scam here, nor that he authorised the payments he made by faster payments to buy genuine cryptocurrency which was then transferred to the scammer via his cryptocurrency account/wallet with S. These transactions (purchasing cryptocurrency) of themselves are not a scam but rather genuine transactions for the genuine purchase of cryptocurrency. The scam happened after that; by Mr A moving his cryptocurrency to the scammer to third parties and to his cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

Whilst we now know circumstances which led Mr A 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 determine whether any of the payments presented an increased risk that Mr A might be the victim of a scam.

I'm also mindful that Revolut can't reasonably be involved in every transaction. There is a balance to be struck between identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments.

In the six months before the scam the account was generally used to send and received payments. Whilst Mr A made payments to various payees regularly the transactions on the account were of relatively low value, he had made larger transactions in the past for example £5,612 on 23 March 2023, £3,000 on 7 March 2023 and one of £2,500 on 7 February 2023. There was also a transaction for £5,500 on 2 December 2022. There was a payment for £7,262 just outside the six months on 11 September 2022.

The initial payment was relatively low in value, and it had been made to a known payee on the account for a year (although it had been a while since Mr A had made a payment and those previous transfer were very low in value). Although Mr A was buying cryptocurrency Revolut had no reason to know this because the money was transferred to S. Whilst S does provide cryptocurrency services it does provide other payment services. As far as Revolut was concerned Mr A was transferring funds to a merchant that provides a variety of payment services – including cryptocurrency.

I think by the time Mr A was transferring a second large sum on the same day – on 29 March 2023 (a total of £11,070 in one day) - Revolut ought to have identified that Mr A might be a risk from financial harm from fraud and stopped the transaction (transaction 3) before processing it.

Combined with the payment earlier that day - it was larger than any other payment that had debited Mr A's account in the previous six months and a pattern of large payments to S was emerging.

I think Revolut would have been aware that the sort code and account number Mr A was transferring his money to was associated with a firm (S) that offers a variety of services, including cryptocurrency and at the time, S was providing payment processing services for a major cryptocurrency firm. So, I don't think Revolut could rule out the possibility that the payments were for cryptocurrency, even if it could not have been sure this was the case. And by March 2023 payments cryptocurrency carried a heightened risk of financial harm from fraud.

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

Revolut initially provided a warning in May 2022 when Mr A first set up S as a new payee. It warned:

*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.*

No further warnings were provided when Mr A made the payments in March 2023.

But this warning wasn't provided in relation to the scam payments at all. And it was provided quite some time before the payments in question and wasn't relevant to the circumstances in which Mr A found himself in. It is very general in nature and it's difficult to see how it would resonate with Mr A or the specific circumstances of the transactions in question (and made quite some time later). I don't think that providing the warning above in relation to an earlier payment was a proportionate or sufficiently specific mechanism to deal with the risk that the third payment presented. I think Revolut needed to do more.

What kind of warning should Revolut have provided?

I've thought carefully about what a proportionate warning in light of the risk presented would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to this one will be entirely genuine. I've given due consideration to Revolut's duty to make payments promptly, as well as what I consider to have been good industry practice at the time this payment was made.

Taking that into account, I think Revolut ought, in line with what I consider to have been good industry practice at the time, as well as what I consider to be fair and reasonable, when Mr A attempted to make Payment 3, to have asked about the purpose of the payment (for example by asking Mr A to select a payment reason from a list of possible reasons) and provided a warning which covered the key scam features of the payment purpose selected.

In March 2023, I think that one of the payment purposes that Mr A could have selected should have covered the key features of cryptocurrency investment scams, given how common they were at the time. I've seen nothing to indicate that Mr A would have not selected the most relevant payment purpose had he been asked.

The warning Revolut ought to have provided should have highlighted, in clear and understandable terms, the key features of common cryptocurrency investment scams, for example referring to: an advertisement on social media, an 'account manager', 'broker' or 'trader' acting on their behalf; fake trading platforms and deals that are too good to be true or warning about being asked to pay fees in order to withdraw investment funds. I recognise that a warning of that kind could not have covered off all the features of a cryptocurrency investment scam. But I think a warning covering the key features of scams affecting many customers, but not imposing a level of friction disproportionate to the risk the payment presented, would have been a proportionate and reasonable way for Revolut to have acted in March 2023 to minimise the risk of financial harm to Mr A.

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

Mr A wasn't given a cover story, so I think Mr A would have answered questions about the payment purpose honestly and answered that he was investing. So, Revolut should, once it had established why Mr A was making the payments, provided a very clear warning tailored to investment scams – including cryptocurrency scams. And if Revolut had given Mr A a tailored warning about cryptocurrency scams, I think Mr A would have recognised his own circumstances in the warnings and quickly realised he was falling victim to a scam.

I think it's very likely that he would have stopped, not followed the fraudster's instructions and his loss would have been prevented.

None of Mr A's other banks flagged any of the payments he made into Revolut or provided warnings. Ultimately, as Revolut didn't ask about the payment purpose for the transactions Mr A made, it can provide no compelling evidence that he would have misled it about the purpose of the payments.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr A 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 A might have been at risk of financial harm from fraud when he made payment 3, 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 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 S does not alter that fact and I think Revolut can fairly be held responsible for Mr A's loss in such circumstances. While I have carefully noted Revolut's comments on this point in response to the view, I am not persuaded to reach a different decision – 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 A has only complained against Revolut. I accept that it's *possible* (although the enquiries made by the investigator suggest that this was not the case) that other firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, and Mr A could instead, or in addition, have sought to complain against those firms. But Mr A has not chosen to do that and ultimately, I cannot compel him to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mr A's compensation in circumstances where: the consumer has only complained about one respondent from which they are entitled to recover their losses in full; has not complained against the other firm (and so is unlikely to recover any amounts apportioned to that firm); and where it is appropriate to hold a business such as Revolut responsible (that could have prevented the loss and is responsible for failing to do so). That isn't, to my mind, wrong in law or irrational but reflects the facts of the case and my view of the fair and reasonable position.

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

Revolut has argued 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. I do not seek to treat Revolut as if it were a signatory to the CRM Code, and I have not sought to apply it by analogy. I've explained in some detail why I think it fair and reasonable that Revolut ought to have identified that Mr A may have been at risk of financial harm from fraud and the steps it should have taken before allowing the payment 3 to leave Mr A's account. And the Financial Ombudsman Service's jurisdiction is neither the same as nor tied to the CRM Code.

Similarly, I consider that it is not 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 payment service provider respectively. They do not preclude me from considering whether Revolut failed to act fairly and reasonably when it made the payment 3 without intervening and providing a warning to Mr A. Revolut does not suggest that I don't have jurisdiction to consider the complaint at all, and in doing so I am required by Parliament and the DISP rules to consider 'all the circumstances of the case'. I am satisfied that if I took the more limited approach Revolut suggests I would not be discharging that duty.

Overall, considering what is fair and reasonable in all the circumstances, I'm satisfied Revolut should have made further enquiries and intervened via its in-app chat to ask Mr A more about the payment purpose and provide warnings about cryptocurrency scams before processing the payment 3. If it had, it is more likely than not that the scam would have been exposed and Mr A would not have lost any more money. In those circumstances I am

satisfied it is fair to hold Revolut responsible for some of Mr A's loss.

### Should Mr A 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'm not going to go into detail here – as Mr A has accepted the investigator's view that a 50% deduction is appropriate. But for completeness I agree broadly for the same reasons. In particular:

Mr A took the word/post of his friend on social media without carrying out much independent research into the investment - other checking online and seeing no negative reviews.

Mr A was promised returns on his investment, which were too good to be true and highly unrealistic.

The messages with the scammer indicate quite early on that Mr A had concerns as he hadn't been told about the need to pay 'withdrawal fees' and 'tax maintenance'. Mr A told the scammer this *'ought to have been clarified from the start'* and after a third request for fees *'this is just getting ridiculous.'*

Despite the constant promises that he'd get his money after one more fee, Mr A made all but the first payment towards fees/taxes to withdraw his money. I think the constant broken promises should have been concerning.

He also queried why the money couldn't be taken from the investment and, in my view, wasn't given a plausible reason as to why that couldn't happen. Yet he continued to make further payments despite the red flags.

Overall whilst I accept Mr A had access to a trading platform which appeared to show his investment growing in real time, there were a number of red flags which ought to have led to Mr A scrutinising the deal more closely, and if he had done, I think he would very quickly have discovered this was a scam.

### **Putting things right**

In order to put things right for Mr A, Revolut Ltd must

- Reimburse 50% of Mr A's loss from payment 3 onwards
- As Mr A has been deprived of the use of this money - pay interest on the above refund calculated at 8% simple per year \* from the date the transactions were made to the date of settlement.

\*If Revolut Ltd considers that it's required by HM Revenue & Customs to deduct income tax from the interest award, it should tell Mr A how much it's taken off. It should also provide a tax deduction certificate if Mr A asks for one, so the tax can be reclaimed from HM Revenue & Customs if appropriate.

### **My final decision**

My final decision is that I uphold this complaint in part, and I require Revolut Ltd to put things right for Mr A as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or

reject my decision before 22 November 2024.

Kathryn Milne  
**Ombudsman**