

## The complaint

Mr O complains that Revolut Ltd (Revolut) is refusing to refund him the amount he lost as the result of a scam.

Mr O is being represented by a third party. To keep things simple, I will refer to Mr O throughout my decision.

## What happened

The background of this complaint is well known to all parties, so I won't repeat what happened in detail.

In summary, Mr O found an advertisement for an investment company online that I will call X. X appeared to be endorsed by a well-known celebrity. Mr O says he decided to make a small investment and later found the investment had been successful.

X told Mr O that if he was to invest more, he would receive a higher rate of return. Mr O agreed and was told to open an account with Revolut. Mr O was also required to download remote access software so X could help him with the investments.

Mr O was able to see the progress of his investment via his account with X on its platform and decided to make a withdrawal. X told Mr O that if he made a withdrawal, he would have to pay tax, and that further investment from Mr O could avoid this.

Mr O still wanted to make a withdrawal, but X stopped responding to him and he later saw his account with X had fallen to £0.00, which is when he realised, he had fallen victim to a scam.

Mr O made the following payments from his Revolut account in relation to the scam:

<u>Payment</u>	<u>Date</u>	<u>Payee</u>	<u>Payment Method</u>	<u>Amount</u>
1	6 February 2023	Global Peak	Transfer	£2,000.00
2	6 February 2023	Skrill	Transfer	£2.00
3	8 February 2023	Skrill	Transfer	£2.00
	9 February 2023	Skrill	Credit	£2.00cr
	9 February 2023	Skrill	Credit	£2.00cr
4	13 February 2023	Binance	Debit Card	£3,590.00
5	13 February 2023	Binance	Debit Card	£1,000.00
6	17 February 2023	Binance	Debit Card	£3,000.00

Our Investigator considered Mr O's complaint and thought it should be upheld in part. Revolut disagreed in summary it said:

- The fraudulent activity did not take place on the Revolut platform, it was just an intermediary link between Mr O's own bank account and the cryptocurrency exchange.

- FOS appears to have decided as a matter of policy, that Revolut should be left “holding the baby” because, subsequent to the self-to-self transfer involving a Revolut account, customers have transferred funds to their own account with a third party. The FOS has concluded those third parties are outside its jurisdiction either because the relevant firm is not authorised, or because the relevant product is not regulated.
- 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.

As an informal outcome could not be agreed this complaint has been passed to me to decide.

### **What I’ve decided – and why**

I’ve considered all the available evidence and arguments to decide what’s fair and reasonable in the circumstances of this complaint.

In 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 O 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;<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 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)<sup>2</sup>.

---

<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\\_further\\_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_further_reduction_in_card_fraud_and_had_offers_from_banks/)

<sup>2</sup> 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.

- 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 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

---

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

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.

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 Mr O was at risk of financial harm from fraud?*

It isn't in dispute that Mr O has fallen victim to a cruel scam here, nor that he authorised the payments he made to purchase cryptocurrency that was subsequently transferred to the scammer.

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

Having said this, I don't think Revolut had reason to intervene when Mr O made the first payments he has disputed as they were relatively low in value and would not have caused Revolut to have concerns. Payment 4 however, was for a much higher value and was being made to a known crypto-currency exchange.

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.

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<sup>4</sup>. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few

---

<sup>4</sup> See for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022. NatWest Group, Barclays, Lloyds Banking Group and Santander had all introduced some restrictions

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 of the above I am satisfied that by the end of 2022, prior to the payments Mr O 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 of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the payments in this case were likely going to an account held in Mr O'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 O might be at a heightened risk of fraud that merited its intervention.

Payment 4 was for a significant value and was being made to a cryptocurrency exchange. Given the increased risk associated with this type of payment I am satisfied that it is fair and reasonable to conclude that Revolut should have intervened before this payment went ahead.

*What did Revolut do to warn Mr O?*

When Mr O made payment 1 he was making a transfer to a new payee and Mr O was provided with warnings relevant to sending funds to a new payee.

Other than this Revolut did not provide any other intervention.

*What kind of warning should Revolut have provided?*

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

Taking that into account, I think Revolut ought, when Mr O attempted to make payment 4, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency scam, without significantly losing impact.

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

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

*If Revolut had provided a cryptocurrency investment scam warning, would that have prevented the losses Mr O incurred after that point?*

I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case. And on the balance of probabilities, I think it would have. There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Mr O's payments, such as the investment being endorsed by a celebrity, being assisted by a broker and being asked to download remote access software.

From the evidence available I don't have enough to say Mr O would have ignored a warning tailored specifically to the type of scam he was experiencing.

Therefore, on the balance of probabilities, had Revolut provided Mr O with an impactful warning that gave details about cryptocurrency investment scams and how he could protect himself from the risk of fraud, I believe it would have resonated with him. He could have for example paused and researched cryptocurrency scams and the celebrity that had endorsed this specific investment. He could also have sought external advice from either a professional or friends and family. I'm satisfied that a timely warning to Mr O from Revolut would very likely have caused him to take additional steps and prevented further loss.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr O made payments into his Revolut account that were then used to purchase cryptocurrency which likely remained in his control before additional steps were required to transfer the funds to the scammer.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr O might have been at risk of financial harm from fraud when he made payment 4, and in those circumstances it should have declined the payment and intervened. If it had taken those steps, I am satisfied it would have prevented the losses Mr O 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 O's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr O'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 O 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 Mr O could instead, or in addition, have sought to complain against those firms. But Mr O 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 O's compensation in circumstances where: he has only complained about one respondent from which he is entitled to recover his 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 O's loss from payment 4 (subject to a deduction for Mr O's own contribution which I will consider below).

*Should Mr O bear any responsibility for his losses?*

Despite regulatory safeguards, there is a general principle that consumers must still take responsibility for their decisions (see s.1C(d) of our enabling statute, the Financial Services and Markets Act 2000).

In the circumstances, I do think it would be fair to reduce compensation by 50% on the basis that Mr O should share blame for what happened.

Having seen an advertisement online supposedly endorsed by a well-known celebrity Mr O appears to have started investing having completed very little due diligence.

Had Mr O carried out a suitable level of due diligence he would likely have found that the celebrity that appeared to endorse the investment had previously publicly warned about investments that appear to be endorsed by them. Mr O could also have found that X was not registered with the FCA.

Had Mr O taken more care I think he would have found red flags that would have caused him to have concerns, and it's likely he too could have prevented his loss.

*Could Revolut have done anything to recover Mr O's money?*

The payments Mr O made in relation to the scam were made using the method of transfer and his debit card.



I can see Revolut attempted to contact the operator of the receiving account for the transfer that took place, but a refund has not been provided.

When Mr O made the payments using his debit card, he was purchasing cryptocurrency that was provided to him in exchange for the payments, I don't consider that a chargeback would have had any prospect of success given there's no dispute that Mr O received the cryptocurrency, which was subsequently sent to the fraudsters.

With the above in mind, I don't think Revolut had any reasonable options available to it to recover the payments Mr O made in relation to the scam.

### **Putting things right**

To put things right I require Revolut Ltd to:

- Refund Mr O 50% of the payments he made in relation to the scam from payment 4 onwards.
- Add 8% simple interest per year to the amount it pays Mr O from the date of the loss to the date the refund is made (less any lawfully deductible tax).

### **My final decision**

I uphold this complaint and require Revolut Ltd to put things right by doing what I've outlined above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr O to accept or reject my decision before 18 April 2025.

Terry Woodham  
**Ombudsman**