

## The complaint

Mr S is unhappy Revolut Ltd won't reimburse him for the money he lost when he fell victim to a scam.

## What happened

Mr S is represented in this complaint by a solicitor, for simplicity I will refer to Mr S throughout this decision, even when referencing what his representatives have said on his behalf.

Mr S saw an investment opportunity online, it offered a low start-up fee and appeared to have been advertised by a popular tv programme. So, Mr S was persuaded it was a good opportunity and decided to leave his contact details. After speaking to what he believed to be genuine investment brokers he agreed to invest in oil and gold. Mr S says he carried out some research of his own and was satisfied that the investment firm he was using was legitimate.

Mr S was encouraged to open an account with Revolut, as well as an account with a third-party cryptocurrency exchange – which I'll call C. The scammers guided Mr S through this process using remote access software. Mr S was also encouraged to take out a loan to fund his investment.

Mr S was then told to make payments into his Revolut account and on to C, from where the funds would be used to make the investments he'd agreed to. Mr S says that he saw some initial small returns on his investment, and so agreed to invest further funds in the scheme. Mr S saw fluctuations in the value of his investments, but overall he believed he was making a reasonable profit. In total Mr S made five payments totalling nearly £24,000, as set out below:

Date	Time	Activity	Amount
21/06/2022	13:25	Faster payment 1	£10
21/06/2022	17:39	Faster payment 2	£4,000
22/06/2022	14:14	Faster payment 3	£4,000
27/06/2022	15:23	Faster payment 4	£10,000
28/06/2022	17:37	Faster payment 5	£5,980.24

Mr S initially asked to withdraw his profits after the third payment made to the scam, but was told he could make higher profits if he invested more. The scammers convinced him to invest a further £10,000. Mr S then asked again about withdrawing his profits. It appears that at this

stage he was told he'd need to make a payment to facilitate that withdrawal. When he made this payment, still did not receive any profits, and the scammers continued to aggressively demand further payments from him – including asking him to send payments via a third party when an attempted payment failed – he realised that something untoward may be going on. He contacted Revolut on 14 July 2022 to tell it what had happened, but ultimately, Revolut told him it would not be able to refund the money he had lost.

Mr S was unhappy with Revolut's response and so he referred his complaint to our service. One of our Investigators looked into what had happened, and they felt that Revolut should have stepped in to question Mr S about the payments he was making by the time of the fourth payment. They felt that, if Revolut had done so, then the scam would have been uncovered and at least some of Mr S' loss could have been prevented. However, the Investigator also felt that Mr S should bear some responsibility for what had happened. They did not consider he had done enough to ensure the firm he was dealing with was legitimate, and felt there were some red flags which should have indicated to him that something may be amiss.

So our Investigator recommended that Revolut refund 50% of the payments made from the fourth payment onwards, plus interest.

Revolut accepted the Investigator's findings, Mr S did not. He maintains that Revolut should have identified that he might be at risk of financial harm at a much earlier stage, and that he had done all he could to check that the investment firm was legitimate.

I have issued two provisional decisions on this case, on 28 September 2023 and on 15 May 2024, explaining that I agreed Revolut should refund some of the payments made, but that I did not consider that any deduction should be made for contributory negligence. So, I recommended that Revolut refund 100% of the payments made from the fourth payment onwards, plus 8% interest.

Mr S accepted my provisional decisions, Revolut said it had no further comments to make in response to my first provisional decision, it has not made any comments in response to my second provisional 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.

In my most recent provisional decision I said the following:

In deciding what's fair and reasonable in all the circumstances of a complaint, I am required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

Having taken all of the above into account, for the reasons I shall set out below, I am minded to conclude that:

- When Mr S attempted to make the fourth payment to the fraudsters – that is the £10,000 payment on 27 June 2022 (Payment 4), Revolut should have recognised that Mr S could be at heightened risk of financial harm from fraud and it should have attempted to establish the circumstances surrounding that payment by, for example, directing Mr S to its in-app chat.

- Once it had established the circumstances surrounding the payment, it should have provided a clear warning to Mr S.
- Had it done so, I think it's more likely than not that Mr S' loss from that payment onwards would have been prevented.
- In those circumstances, I consider it to be fair and reasonable to hold Revolut responsible for Mr S's loss.

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*<sup>1</sup>, 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.
- The express terms of the current account contract may modify or alter that position. For example, 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 duty to do so.

In this case, the terms of Revolut's contract with Mr S at the time did expressly require it to refuse or delay a payment for a number of reasons. Those reasons included "*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 S and the Payment Services Regulations to carry out his 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 in Mr S' case, 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>2</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> [2023] UKSC 25

<sup>2</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 June 2022 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 that view, 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>3</sup>
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system; and
- 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:

- FCA regulated banks are required to conduct their “business with due skill, care and diligence” (FCA Principle for Businesses 2) and to “pay due regard to the interests of its customers” (Principle 6)<sup>4</sup>.
- Over the years, the FSA, and its successor the FCA, 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 here, but I nevertheless consider these requirements to be relevant to the consideration of a firm’s obligation to monitor its customer’s accounts and scrutinise transactions.
- The October 2017, BSI Code<sup>5</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) and it has since been withdrawn, but the standards and

---

<sup>3</sup> For example, Revolut’s website explains it launched an automated anti-fraud system in August 2018:

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

<sup>4</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.

<sup>5</sup> BSI: PAS 17271: 2017 “Protecting customers from financial harm as result of fraud or financial abuse”

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 the practices articulated in the BSI Code remain a starting point for what I consider to have been the minimum standards of good industry practice in January 2023 (regardless of the fact the BSI Code was withdrawn in 2022).

- By June 2022, firms like Revolut ought to have been aware of the risk of multi-stage scams involving cryptocurrency. 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 multi-stage scams involve the use of EMI's (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

Overall, taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Revolut should fairly and reasonably in June 2022:

- 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 financial harm from 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;
- 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 S was at risk of financial harm from fraud and were any steps taken to warn him?*

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

Whilst I have set out in some detail in this provisional decision the circumstances which led Mr S 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 Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Mr S might be the victim of a scam.

I'm aware that cryptocurrency exchanges like C 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 send and receive cash payments from the exchange. Revolut would have been aware of this fact. So, it could have reasonably assumed that all of the payments in question were made to an account in Mr S' own name.

I also accept that, as a general starting proposition, a firm might reasonably conclude that payments made between accounts under a customer's control might be expected to carry a lower fraud risk. That might particularly be the case where a payee or recipient is well-known and long-standing. But while a firm may be able to take a certain level of reassurance when its customer is paying an account in their own name, given the prevalence of multi-stage fraud, it cannot reasonably rule out the possibility of a scam simply because the payment is going to the customer's own account.

By the time Mr S fell victim to this scam, firms like Revolut ought to have been aware of the risk of multi-stage scams involving cryptocurrency. I am also mindful that 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 have continued to increase since. It is also worth noting that one well-documented feature of some cryptocurrency scams is fraudsters having complete or considerable control over cryptocurrency accounts which are (sometimes only nominally) held in a victim's name.

So, Revolut ought fairly and reasonably to have recognised that its customers could still be at risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name. In those circumstances, as a matter of what I consider to have been fair and reasonable and good practice, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments.

Taking all of the above into account, I don't think the fact that the payments in this case were going to an account held in Mr S' own name should have led Revolut to believe there *wasn't* a risk of fraud.

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

*Should Revolut have identified that Mrs M might be at a heightened risk of fraud?*

As I explained in my first provisional decision, Mr S' Revolut account was opened at the instruction of the scammers, so it was a new account with no previous transaction history for Revolut to compare payments to. The first three payments made by Mr S were for £10, £4,000 and £4,000 and were made over a couple of days. I appreciate that Mr S feels these payments should have been flagged as unusual by Revolut, but given that it had no transaction history for Mr S' account, Revolut would have been relying on more generic indicators of fraud risk. Revolut would have had no idea of what might be normal for Mr S' account at that time. I do appreciate that £4,000 feels like a lot of money, and that two payments of this amount were made over the course of only two days, which could have suggested the start of a pattern of potentially suspicious payments. However, given the individual value of the payments, and the limited account history it was working with, I don't think there was enough going on at this stage to have triggered further questions from Revolut. So I consider that Revolut acted reasonably in allowing these payments to be made without further questioning.

I do though think that Payment 4 should have flagged as potentially suspicious to Revolut. This amount was more than double the previous payments Mr S had made and showed that a pattern was emerging of large payments being made into the account and then quickly paid out again. In my view, this fourth payment marked a clear escalation in value and had the potential to cause significant financial harm to Mr S. Given the circumstances of Payment 4, taken together with the earlier payments, I consider Revolut ought reasonably to

have identified that a pattern had developed – of increasingly large payments to a cryptocurrency provider – that could indicate Mr S was at risk of financial harm from fraud.

So, when Mrs M attempted to make Payment 4, I think Revolut ought fairly and reasonably to have recognised the risk had increased and there was a heightened possibility that the transaction could be linked to a scam.

*What should Revolut have done in response to the risk presented by the fourth payment?*

I acknowledge that Revolut says it provided a general warning regarding the risk of scams when Mr S sent each transfer, specifically it says this warning asked if Mr S trusted the person he was sending the funds to. But I don't think this kind of warning would have flagged to Mr S that he might be at risk, given that it didn't provide any specific information about scams that would have resonated with Mr S and that in any case, he believed he could trust the account he was paying – it was after all an account that he had opened at C himself.

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 S attempted to make Payment 4, to have attempted to establish the circumstances surrounding this payment before allowing it to debit Mr S' account.

*If Revolut had attempted to establish the circumstances surrounding Payment 4, would the scam have come to light and Mr S' loss from that point on been prevented?*

I've considered this point carefully. Mr S has told us he was not given any cover story to use regarding the payments he was making, so I consider it very likely that, had Revolut asked him, Mr S would have been open and honest about what he was making the payments for – payments to cryptocurrency for an investment. And what Mr S would likely have told Revolut about what he was doing should have rung alarm bells for Revolut, given that it would have been aware, by that stage, of the risk cryptocurrency scams represented. Specifically, Mr S had found the investment opportunity on social media, had been asked to download remote access software by the scammers, hadn't been able to withdraw any profits, and was communicating with the scammers via a messaging app, which would not be normal behaviour for a legitimate investment firm. Revolut could then have explained the risk Mr S was exposing himself to, including explaining some of the common features of investment scams – many of which, such as the use of remote access software, would have resonated with Mr S.

I note that Mr S first transferred funds into his Revolut account from an account he held with another bank – B – before moving them on to C. But B has told us it has no evidence of any intervention in the payments from its side. So, I can't see that Mr S ignored any interventions regarding the payments he was making.

So I think, on the balance of probabilities, that appropriate intervention from Revolut is likely to have caused Mr S to stop making payments to the scam. I can see no reason for him to have continued to make the payments if he was presented with an appropriate warning.

I'm therefore satisfied that had Revolut established the circumstances surrounding Payment 4, as I think it ought to have done, and provided a clear warning, Mr S' loss from and including Payment 4 would have been prevented.

*Is it fair and reasonable for Revolut to be held responsible for some of Mr S' loss?*

In reaching my decision about what is fair and reasonable I have taken into account that Mr S' Revolut account was funded by payments from B (another regulated business) and Mr S might potentially have a claim against B in respect of its actions (although B is not a party to this complaint and so I make no finding about its role here). As noted, B has been contacted as part of the investigation into this complaint in an attempt to gather evidence relevant to the outcome.

But whilst the dispute resolution rules (DISP) give me the power (but do not compel me) to require a financial business to pay a proportion of an award in circumstances where a consumer has made complaints against two financial businesses about connected circumstances, Mr S has not referred a complaint about B to me and DISP does not empower me to instruct Mr B to make or refer a complaint to me about another business.

I have also taken into account that Mr S paid money using his Revolut account to another account in his own name at C, rather than directly to the fraudster, so he remained in control of his money after he made the payments, and there were further steps before the money was lost to the scammer.

But for the reasons I have already set out in this decision, I am satisfied that it would be fair to hold Revolut responsible for Mr S' losses from (and including) Payment 4. As I have explained, the potential for multi-stage scams, particularly those involving cryptocurrency, ought to have been well known to Revolut. And as a matter of good practice, I consider it fair and reasonable that Revolut should have been on the look-out for payments presenting an additional scam risk including those involving multi-stage scams.

*Should Mr S bear any responsibility for his loss?*

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

Having considered the matter carefully, I don't think that there should be any deduction from the amount reimbursed.

Mr S has said he carried out searches for reviews of the investment company, and I've done a similar search. I can see that, at the time the fraud took place, there were numerous positive reviews for the investment firm, and I've not found anything that would have suggested to Mr S at the time that the company he was dealing with was not legitimate. The website of the investment firm looks professional and doesn't ring any immediate alarm bells. I note that Mr S didn't have any written confirmation of his agreement with the firm, but I don't think that would have been enough to flag to him that he might be at risk, particularly given that an increasingly large number of legitimate accounts for savings and investments are opened up without a signed contract. I also note that, when viewing his investments – on what appeared to be a legitimate trading platform – Mr S was seeing relatively modest profits (and some losses) which would have added to his belief that this was a legitimate investment scheme. I've not seen anything to suggest that he was offered returns that could be considered too good to be true.

I do appreciate that the last payment Mr S made to the scam was apparently a payment to enable the withdrawal of his profits, and I think this should reasonably have been considered



unusual by Mr S, and ought to have prompted him to have some concerns that the scheme might not have been genuine. My finding in relation to contributory negligence is more finely balanced in relation to this payment than in relation to Payment 4. But, as I've set out, taking together Mr S' knowledge and experience as well as the limited information available at the time about the company he was dealing with, it would have been relatively difficult for Mr S to uncover the scam at this point.

I acknowledge that Mr S did start to believe he'd been scammed after there were further demands for payment but at that point, I understand the fraudster's demeanour changed and, of course, they had still not allowed Mr S to withdraw his money following the previous payment. I think those facts gave Mr S a much more compelling reason to believe that he was the victim of a scam and I think he acted reasonably by not making any further payments.

Given this background, I don't think Mr S was partly to blame for what happened here. It follows that I don't consider it fair to say Mr S should bear responsibility for some of his financial loss.

#### *Could Revolut have done anything else to recover Mr S' money?*

I've also thought about whether Revolut could have done more to recover the funds after Mr S reported the fraud.

The Faster Payments were sent to Mr S' own account at C, converted into cryptocurrency and then sent to the fraudster. So, though Revolut did attempt to recover those payments, in these circumstances, it's difficult to see how any recovery would have been possible. So I don't think there was anything more Revolut could've done to recover the money in these circumstances.

So, in summary, I consider when Mr S made Payment 4, Revolut could have done more to protect him from the risk of financial harm. Had Revolut contacted Mr S directly and asked some open questions about what was happening, I'm persuaded it is more likely than not the scam would have come to light, and Mr S wouldn't have lost out on the £15,980.24 he then went on to transfer. So, I consider it fair and reasonable for Revolut to refund that amount to Mr S, along with interest at our standard compensatory rate of 8%, and I don't consider that Mr S' actions contributed to his loss, so I won't be making any deduction from that amount.

Given that Mr S has accepted my findings, and Revolut has not made any comments in response to what I have said above, I see no reason to depart from the findings I have previously set out. I remain satisfied that Revolut should refund the last two payments Mr S made to the scam, plus interest.

#### **Putting things right**

To resolve this complaint Revolut should:

- Refund payments 4 and 5 to Mr S (representing a refund of £15,980.24, Revolut can deduct any sums that have already been refunded, or that have been recovered and subsequently returned to Mr S).
- Pay 8% simple interest per annum on this amount, calculated from the date of each payment until this complaint is settled.

**My final decision**

I uphold this complaint in part. Revolut Ltd should now put things right in the way I've set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 15 July 2024.

Sophie Mitchell  
**Ombudsman**