

The complaint

Mr F is unhappy that Revolut Ltd (“Revolut”) won’t refund him the money he lost as a result of a cryptocurrency scam.

What happened

Mr F told us that in September 2022 he was looking at a website and he saw an advert for an investment opportunity and clicked on a link to provide his contact details. He says he was then contacted by a company - I will refer to as P in this decision. Mr F says P initially told him the average return would be 12% per month. Mr F says he was told to open the Revolut account as part of the scam. He said when he doubled the value of his investment, P changed the trading strategy to a riskier approach. Mr F says when he asked to withdraw his money, P kept asking him for more money for fees to withdraw his funds. As a result, Mr F made the following transactions:

Date	Credit	Debit	Payee
14/09/2022		£10	Cryptocurrency C
14/09/2022		£10	Mr F’s W account
16/09/2022		£2,100	Cryptocurrency C
18/09/2022		£2,125	Cryptocurrency C
19/09/2022		£3,550	Cryptocurrency C
03/10/2022		£5,000	Cryptocurrency C
12/10/2022		£3,075	Cryptocurrency C
10/11/2022		£17,500	Cryptocurrency C
25/11/2022		£4,235	Cryptocurrency C
29/11/2022		£2,260	Cryptocurrency C

The money went from Mr F’s Revolut account to an account in his own name with a cryptocurrency provider. This is where he purchased cryptocurrency which went into a wallet in Mr F’s own name. He then sent this on to P. He had access to a fake trading platform which appeared to show his investment growing in real time.

Prior to these transactions, Revolut declined a number of transactions Mr F was attempting to make to one of his other bank accounts (bank W). And when he entered the payment purpose as ‘safe account’ it triggered Revolut to pause the payment and find out more. Revolut also asked if Mr F had been asked to install any remote access applications. Mr F did not respond. Revolut then paused another attempted payment (for the same payment purpose) and again asked Mr F whether he’d been asked to install any remote access applications. Mr F initially responded that he just wanted to transfer his money back to his W account. And eventually told Revolut he had removed the remote access application. Then the transactions to cryptocurrency began. After a couple of months of making the payments, Mr F realised he had been scammed and reported the matter to Revolut.

Revolut recovered £10 from Mr F’s W bank account and £115.54 from his cryptocurrency provider. However, it declined to provide a refund.

Our investigator upheld the complaint in part. She felt Revolut should have asked further questions when it paused the payments prior to the disputed transactions starting. But she also considered Mr F should share in the responsibility for his losses - so recommended Revolut refund 50% of all the transactions.

Mr F accepted the investigator's conclusions, Revolut didn't agree. I've read all of its submissions but in summary it said:

- 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 20 November 2024 explaining why I was reaching a slightly different outcome to the investigator. Mr F accepted my provisional decision. Revolut didn't respond.

What I've decided – and why

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

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 F 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 F 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 immediately¹. 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.

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 September 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 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;²
- 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”*.

¹ 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).

² 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/>

- 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 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.

Overall, taking into account relevant law, regulatory rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in September 2022 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.

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

It isn't in dispute that Mr F 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 C. 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 F moving his cryptocurrency from his wallet and transferring it to the scammer's wallet).

Whilst we now know the circumstances which led Mr F to make the payments using his newly opened 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 F might be the victim of a scam.

Buying cryptocurrency is a legitimate activity and the payments were made to a genuine cryptocurrency exchange. The payments were also to an account in Mr F's own name. I appreciate the loss happened from Mr F's cryptocurrency account, but Revolut ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it ought to have done more when Mr F tried to make the payments.

Mr F opened the Revolut account on 12 September 2022. Revolut did reach out to Mr F before he started making payments to cryptocurrency C. It was concerned about the payment purpose he selected when transferring money to his own account with bank W. It was also concerned whether he had installed a remote access application. But I think Revolut could be reassured that Mr F was genuinely moving money back to his own account elsewhere given his responses in Revolut's in app chat function and the incoming payment of £1,800 from Mr F's own account with bank W that preceded this activity.

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. And I think the first few payments to cryptocurrency C were relatively low value (although I appreciate it is a lot of money to Mr F).

But by the £3,550 payment on 19 September 2022 there was a noticeable uplift in the value of the amounts being sent after just a few days. And Mr F had also started transferring money back to Revolut from his Bank W account to fund the onward payments to cryptocurrency (contradictory to the conversations he had had with Revolut only a few days earlier). I think by this point the pattern of payments and the increase in values were consistent with a risk of financial harm. Given Revolut's earlier interactions with Mr F and concerns over remote access installation coupled with the fact that he'd also told them the transfers to C were connected with an investment. Overall, I'm persuaded the activity on the account since its opening ought reasonably to have appeared suspicious to Revolut and it ought to have intervened here, before allowing any further payments to be made.

Revolut would have been aware at the time that fraudsters use genuine firms offering cryptocurrency as a way of defrauding customers. Cryptocurrency scams had been increasing in frequency and both the Financial Conduct Authority (FCA) and Action Fraud had published specific warnings about these scams in 2018. In my view, by the time of these transactions, Revolut had had time to understand these warnings and put mechanisms in place to detect and prevent this particular type of fraud.

So, it may have appeared on face value to have been legitimate payments to a legitimate organisation. But even though the money appeared to be going somewhere safe or on (as it did) to the consumer's own wallet, I don't think the conversation should have stopped there. Based on the industry warnings at the time, I think Revolut ought to have had a good enough understanding of how these scams work – including that consumers often move money to buy genuine cryptocurrency before moving it on again to a fraudster.

What did Revolut do to warn Mr F?

Revolut initially provided a warning when Mr F first set up C as a new payee and tried to transfer £100 on 13 September. 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.

It also asked Mr F a series of questions. In his response, Mr F said he was investing. This was also in line with the account opening purpose to 'spend or save money'. Although this particular payment didn't go ahead – a smaller amount for £10 was successfully transferred the following day. Revolut hasn't indicated it gave a warning (in response to the series of questions) at this stage.

No further warnings or intervention took place. But by the time Mr F made the £3,550 payment, 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 F attempted to make the £3,550 – bearing in mind the risk it presented, 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 F's account. I think it should have done this by, for example, directing Mr F to its in-app chat to discuss the payment further before processing it.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr F suffered from the £3,550 payment?

I've thought about whether it would have been reasonable for Revolut to uncover the facts that subsequently came to light.

Mr F wasn't given a cover story and was open and honest about the fact he was 'investing' when initially asked by Revolut. So if Revolut had asked open questions and probed further about the cryptocurrency investment Mr F was making for example; who he was paying his cryptocurrency to, how he had been contacted, and whether he'd opened a trading account, I think Mr F would have told Revolut about P. I think Mr F would have explained P had contacted him after he'd seen an advert online and were promising returns of 12% per month. With further questioning, I think Revolut would have been on notice that Mr F was falling victim to a scam. And if Revolut had given Mr F some warnings about cryptocurrency scams including pointing out that scam firms can manipulate software to distort prices and returns and scam people into buying non-existent currency – I think this would have caused sufficient doubt in Mr F's mind not to proceed with the payments. In other words, if Revolut had carried out further or better questioning in line with its duty of care, it seems probable that Mr F would have become credulous about the scam in time and stopped the £3,550 payment (and any subsequent payments) in its tracks. The fraud would have failed; and Mr F would not have lost £3,550 or the transactions that followed.

None of Mr F'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 F 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 F's loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Mr F 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 F might have been at risk of financial harm from fraud when he made the £3,550 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 F 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 C does not alter that fact and I think Revolut can fairly be held responsible for Mr F'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 F 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 F could instead, or in addition, have sought to complain against those firms. But Mr F 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 F'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 F's loss from the £3,550 (subject to a deduction for Mr F'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 F may have been at risk of financial harm from fraud and the steps it should have taken before allowing the £3,550 payment to leave Mr F'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 £3,550 payment without intervening and providing a warning to Mr F. 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 F more about the payment purpose and provide warnings about cryptocurrency scams before processing the £3,550 payment. If it had, it is more likely than not that the scam would have been exposed and Mr F would not have lost any more money. In those circumstances I am satisfied it is fair to hold Revolut responsible for some of Mr F's loss.

Should Mr F 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 F 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 F has sent some screen shots of the fake investment platform and I can understand this was a convincing element. I understand there was an FCA warning about P – but this was quite some time into the scam and there was no reason for Mr F to necessarily have checked things out further once caught up in the scam.

However, without the full messages between Mr F and the fraudster, it's difficult for me to establish what led Mr F to believe this was a genuine situation or whether the reasoning for the payment requests was plausible.

From the very limited messages between Mr F and the scammer - very few of those seem to relate to the scam itself or the payments made. The ones I've seen (and have been translated) don't appear professional or how I would expect a legitimate organisation to communicate with an investor.

Mr F also says he was promised returns on his investment of 12% per month, which were too good to be true and highly unrealistic.

Overall, and on balance, it is very difficult for me to determine how Mr F was led to believe that this was a genuine situation or how he was persuaded to make the various payments. Certainly, by the time of the transaction I am upholding from I think ought to have been questioning things further. So I think it fair for any refund to be reduced by 50%.

Putting things right

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

- Refund Mr F's loss from the £3,550 onwards less the recovered funds Revolut returned to Mr F
- Reduce the above sum by 50%
- As Mr F 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 F how much it's taken off. It should also provide a tax deduction certificate if Mr F 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 F as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr F to accept or reject my decision before 6 January 2025.

Kathryn Milne
Ombudsman