

The complaint

Mr V complains that Revolut Ltd has declined to reimburse payments he made as part of an investment scam.

What happened

As the facts are well known to both parties and not in dispute, I'll summarise them briefly.

Mr V found an investment opportunity on social media that appeared to be endorsed by a well-known public figure. He registered his interest on its website, and was then contacted by an 'adviser' who explained that he would need to deposit funds which an account manager would then trade with. Mr V was also told to download messaging apps and remote access software so the company could communicate with him and assist him in investing.

After Mr V initially invested 100 Euros from another account, the scammer helped him to withdraw his profit – this was a credit of £13.24 to his Revolut account on 27 February 2023. He then made further payments towards his investment and was then told that the market went in the wrong direction and that he needed to close the platform to withdraw his funds. The scammer then persuaded Mr V that there were different reasons for issues doing this, including telling him that he had made an error which affected the bank being able to legally send his money and his trading account was frozen. He was told to send further funds to help with this which is what the payment on 28 March 2023 relates to.

Here is a list of the disputed payments – they are all debit card payments to the same cryptocurrency platform. (Some of the payments were in Euros but for simplicity I've included the amount in GBP that left Mr V's account.)

Payment no.	Date	Amount
1	27/02/2023	- £907.00
2	10/03/2023	- £2,953.00
3	22/03/2023	- £4,873.00
4	23/03/2023	- £3,539.00
5	23/03/2023	- £4,424.00
6	25/03/2023	- £4,817.00
7	25/03/2023	- £4,000.00
8	28/03/2023	- £6,341.00

Revolut declined to reimburse Mr V on the basis that the payments were authorised, and that Mr V would not have had chargeback rights as the service had been provided by the merchant.

When Mr V referred his complaint to our service via a professional representative, they argued that Revolut ought to have identified the payments as higher risk and intervened. They say that an effective warning would have revealed the scam and prevented Mr V's

loss.

Revolut in its submission to our service said:

- All transactions were initiated and authorised by Mr V. The transactions were 3DS authenticated and there were no signs of an account takeover.
- The transactions were money orders.
- The merchant is a well-known cryptocurrencies services provider and the funds were sent out of the merchant's website.
- The fraudulent activity did not take place primarily on the Revolut platform. Mr V sent the funds to an account he held with the cryptocurrency platform and subsequently lost control of the funds further in the chain;
- Unrealistic returns were not questioned by Mr V;
- Mr V showed a lack of appropriate due diligence;
- The scam was not a 'heat of the moment' single payment or 'out of character' transaction scenario, but a scam where eight payments were sent over a period of one month.

The investigator upheld the complaint – they thought it would be fair for Revolut to reimburse 50% of payment 3 onwards.

Mr V accepted this, but Revolut didn't agree. In summary it said:

- Revolut doesn't owe a duty to prevent fraud and scams.
- Reimbursement codes and rules don't generally apply to Mr V's payments which are self-to-self transactions.
- Mr V failed to conduct due diligence and his carelessness displaces Revolut's liability.
- It is relevant if other banks or institutions intervened.

As an agreement couldn't be reached, the matter was passed to me for consideration by an ombudsman. I asked Mr V for further information to clarify what Mr V thought each payment was for, the source of funds, and evidence of loss. I then issued a provisional decision on 14 April 2025 explaining why I intended on upholding the complaint but with different redress to the investigator.

Mr V accepted my provisional decision, and Revolut acknowledged receipt. Revolut confirmed it had nothing further to add but appears to still be requesting a final decision on the matter.

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.

As no new evidence or information has been provided in response to my provisional decision, my findings remain the same. I'm upholding this complaint and making a partial award for Mr V's losses.

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 V 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 / March 2023 have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

In reaching the view that Revolut should have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances, I am mindful that in practice all banks and EMI's like Revolut did in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;¹
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system for authorised push payments;
- providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified.

For example, it is my understanding that in February / March 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat).

I am also mindful that:

- Electronic Money Institutions like Revolut are required to conduct their business with “due skill, care and diligence” (FCA Principle for Businesses 2), “integrity” (FCA Principle for Businesses 1) and a firm “must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems” (FCA Principle for Businesses 3)².
- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the *“Financial crime: a guide for firms”*.
- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I 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

¹ For example, Revolut's website explains it launched an automated anti-fraud system in August 2018: <https://www.revolut.com/news/revolut-unveils-new-fleet-of-machine-learning-technology-that-has-seen-a-fourfold-reduction-in-card-fraud-and-had-offers-from-banks/>

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

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

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 / 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.

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 / March 2023, Revolut should in any event have taken these steps.

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

It isn't in dispute that Mr V has fallen victim to a cruel scam here, nor that he authorised the payments he made to his cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer). Whilst I have set out the circumstances which led Mr V 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 V might be the victim of a scam.

By February / March 2023, when the third payment 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 transactions⁴.

This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry. I recognise that, as a result of the actions of other payment service providers, many customers who wish to purchase cryptocurrency for legitimate purposes will be more likely to use the services of an EMI, such as Revolut. And I'm also mindful that a significant majority of cryptocurrency purchases made using a Revolut account will be legitimate and not related to any kind of fraud (as Revolut has told our service). However, our service has also seen numerous examples of consumers being directed by fraudsters to use Revolut accounts in order to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider, a fact that Revolut is aware of. So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mr V made in February / March 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 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 / March 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

⁴ See for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022.

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 fact the payments in this case were going to an account held in Mr V'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 V might be at a heightened risk of fraud that merited its intervention.

Should Revolut have identified that Mr V might be at a heightened risk of fraud and if so, what kind of warning should Revolut have provided?

Having considered the disputed scam payments, I don't think that Revolut ought to have intervened in the first two payments. This is because they were for relatively low value, and they were made two weeks apart.

However, payment three was for a higher value and so given it was also identifiable to a cryptocurrency platform, I think that the circumstances should have led Revolut to consider that Mr V was at a heightened risk of financial harm from fraud. And so, I am satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this payment went ahead.

To be clear, I do not suggest that Revolut should apply significant friction to every payment its customers make to cryptocurrency providers. However, for the reasons I've set out above I'm satisfied that by March 2023 Revolut should have recognised at a general level that its customers could be at increased risk of fraud when using its services to purchase cryptocurrency and, therefore, it should have taken appropriate measures to counter that risk to help protect its customers from financial harm from fraud. Such proportionate measures would not ultimately prevent consumers from making payments for legitimate purposes.

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 V attempted to make the 22 March 2023 payment, knowing 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 V by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

However, I'm not persuaded that this would have prevented Mr V's loss. I say this because Mr V thought he was investing in currencies and commodities, not cryptocurrency. And that he needed to do this via his account with the cryptocurrency platform. He had also received some profit and says he was making this payment (payment three and subsequent payments) for errors made while trading and to access profits made. Rather than to further invest. So, I don't think a written warning detailing the key features of a cryptocurrency investment scam would have been similar enough to what he thought he was doing to have resonated with him or persuaded him not to make further payments. I also think this would be the case at payment four.

By payment five, I think the payments had escalated establishing a heightened risk consistent with known patterns of fraud. Mr V had made a payment the previous day and earlier that day, making this the third payment to cryptocurrency in two days. Having thought carefully about the risk payment 5 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 V's account. I think it should have done this by, for example, directing Mr V to its in-app chat to discuss the payment further.

Had Mr V told Revolut that the payments were to help him access his profits on an investment he had made or to pay for an error he had made, I think Revolut would have (or ought to have) immediately recognised that he had fallen victim to a scam. Particularly given he was told he needed to use a cryptocurrency platform to purchase commodities in Euros, which Revolut would have known wasn't normal practice. There were other factors present as well, such as the name of the scam trading platform which had a live FCA warning added on 16 March 2022 that also would have helped to identify the scam and persuade Mr V not to continue making payments. I haven't seen anything to suggest that Mr V wouldn't have been honest in response to any questions by Revolut to have prevented this. I'm also not aware that any interventions did take place with Revolut or other businesses. So, I think on the balance of probabilities, that's likely to have caused Mr V to stop.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr V credited his Revolut account from other accounts and then sent the payments from Revolut to genuine cryptocurrency sellers – who credited Mr V's wallets with cryptocurrency that was sent on to the scam. While I appreciate he was being guided by the scammers, I think there were further steps taken before it was lost to the scam. That is because I have seen he had access to his wallet held with the cryptocurrency platform.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr V might have been at risk of financial harm from fraud when he made payment five, 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 V 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 Mr V's own account does not alter that fact and I think Revolut can fairly be held responsible for his 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 V has only complained against Revolut. I accept that it's *possible* that other firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, and consumer could instead, or in addition, have sought to complain against those firms. But Mr V 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 not persuaded it would be fair to reduce a consumer'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 consumer's loss from payment five (subject to a deduction for consumer's own contribution which I will consider below).

Should consumer bear any responsibility for their losses?

I can see why Mr V initially found the scam convincing, though he only undertook a basic search of the company at the time. I recognise that there were relatively sophisticated aspects to this scam, not least an apparently credible and professional looking platform.

Mr V initially said that when he researched the company, he saw both positive and negative reviews. And that when he discussed this with the scammer he was told some people who lose money on investments aren't happy.

I think Mr V ought to have been concerned when he was asked to make further payments to be able to access his account and withdraw his profits. He was given several varying reasons for these payments, such as that his account had been frozen and that he had made mistakes such as trading too high. New costs were introduced, and he was given inconsistent information about the percentages he needed to pay for "restricting tariffs" and the legal support for his withdrawals. Whilst Mr V hasn't said what profit he thought he was making for me to assess how realistic these were, the payments he thought he needed to make for his errors and to withdraw his profits significantly outweighed the amount he had invested. I don't think from his explanation of events that it was reasonable to find these plausible. I therefore think it would have been reasonable for Mr V to have stopped or taken steps to reassure himself of the legitimacy of the company and costs he was being asked to pay. Had Mr V researched the company or reasons he'd been given to make the payments more thoroughly, he would likely have seen that these weren't legitimate reasons and that an FCA warning was added about the company on 16 March 2022.

I've concluded, on balance, that it would be fair to reduce the amount Revolut pays Mr V because of his role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

Was there anything else Revolut should have done to recover Mr V's loss?

The payments were made by card to a cryptocurrency provider, to an account held by Mr V. The funds were then sent on from that platform to the fraudsters. So, Revolut would not have been able to recover the funds. In addition, I don't consider that a chargeback would have had any prospect of success given the limited grounds for a chargeback. There's no dispute that the cryptocurrency platform provided cryptocurrency to Mr V – and therefore the merchant would be able to demonstrate that it had provided the goods/services that had been purchased.

Putting things right

For the reasons I've explained, I think Revolut should reimburse Mr V 50% of payments five to eight.

I'm mindful that some of the money Mr V lost to the scam was borrowed from third parties which he's now repaid, and that some of the funds credited to the account were being repaid to him by third parties. But I'm satisfied that based on what I've been provided with that it's likely he has suffered a loss higher than I am awarding. And as he hasn't had use of these funds, I think it's fair for Revolut to pay Mr V simple interest at a rate of 8% on the amount awarded.

My final decision

My final decision is that Revolut Ltd should reimburse Mr V 50% of payments five to eight.

It should also pay Mr V simple interest at a rate of 8% from the date of the payments to the date of settlement.

If Revolut Ltd considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Mr V how much it's taken off. It should also give Mr V a tax deduction certificate if he asks for one.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr V to accept or reject my decision before 29 May 2025.

Stephanie Mitchell
Ombudsman