

The complaint

Mr C complains that Revolut Ltd did not reimburse the funds he lost to a scam.

What happened

Mr C found an investment opportunity on social media, which he thought his daughter was recommending, however her social media account had been taken over by scammers. Mr C signed up after seeing lots of positive reviews online about the company and was assigned a financial advisor. He began trading in cryptocurrency via his Revolut account and a cryptocurrency wallet, which he used to send funds to the investment. His portfolio grew and he saw returns on the platform.

Due to bad reviews for the company, his financial advisor left the company he initially invested in, and Mr C stayed with the financial advisor. Over time, his returns grew and he eventually attempted to withdraw his funds, however he was told he had to pay fees in order to do so. At that point, Mr C realised he had been the victim of a scam and raised a scam claim with Revolut. He made the following card payments from his Revolut account to his cryptocurrency wallet:

Date	Amount
08/12/2022	1,000.00 GBP
07/02/2023	900.00 GBP
31/03/2023	500.00 GBP
18/07/2023	3,000.00 GBP
28/07/2023	1,500.00 GBP
18/08/2023	3,900.00 GBP

Revolut issued a final response letter in which they explained they would attempt a chargeback claim for the card payments, but there was no guarantee of success. They later confirmed the chargeback claims were unsuccessful and did not agree to reimburse Mr C.

Mr C referred the complaint to our service and our Investigator looked into it. They felt that the payment of £3,000 to a known cryptocurrency merchant should have been stopped and Revolut should have provided Mr C with a tailored cryptocurrency warning. As Mr C's complaint had the hallmarks of a scam, they felt a clear warning highlighting these would have been enough to reveal the scam at that point and prevent further payments from being made. They recommended a full refund from the payment of £3,000 onwards, plus 8% simple interest.

Mr C accepted the findings however Revolut did not. In summary, they highlighted the funds were forwarded from the Revolut account to another account in Mr C's control, so they did not agree they were the point of loss. As an informal agreement could not be reached, the complaint has been passed to me for a final 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 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 C 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 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 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.

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.

- 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.
- 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 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.

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

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 at the time, Revolut should in any event have taken these steps.

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

It isn't in dispute that Mr C fell victim to a cruel scam, nor that he authorised the payments to his cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

By early 2023, when the majority of these transactions took place, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency for some time. Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions.

By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions. And by early 2023, when the majority of these payments took place, further restrictions were in place. 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, 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.

In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments.

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 most of the payments in this case were going to an account held in Mr C'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 C might be at a heightened risk of fraud that merited its intervention. I can see that Mr C opened the Revolut account in order to facilitate the payments to the scam. Because of this, there was no previous genuine account

activity to compare the scam payments to.

On balance, I don't think the initial three payments were unusual enough to warrant an intervention from Revolut. They were not of a particularly high value, and they were relatively spaced out over a few months. However, I do think the payment of £3,000 was unusual enough to warrant intervention from Revolut prior to it being processed. It was identifiably going to a known cryptocurrency provider, which as explained above carried its own increased risk level. And I think it was of a significant enough value that it posed a level of risk that required an intervention. In line with good industry practice and regulatory requirements I am satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this payment went ahead.

What did Revolut do to warn Mr C?

Revolut has said that it carried out 3DS authorisation on the card payments, meaning Mr C had to go through an additional layer of security to authorise the payments. While this ensures Mr C is the one who authorised the payments, it does not specifically protect against authorised push payment scams.

I can also see that in September 2023, following the scam payments listed above, Mr C attempted to make further card payment to his cryptocurrency wallet for £1,440, however this was declined by Revolut due to fraud concerns. He was referred to the in-app chat for some questions, however the conversation did not continue for long and soon both parties stopped communicating. This payment was not re-attempted by Mr C and no further payments were made towards the scam.

What kind of warning should Revolut have provided?

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

Taking that into account, I think Revolut ought, when Mr C attempted to make the £3,000 payment on 18 July 2023, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency scam, without significantly losing impact.

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

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

If Revolut had provided a warning of the type described, would that have prevented the losses Mr C suffered from the £3,000 payment?

On balance, I think it is more likely a tailored cryptocurrency investment scam warning on the payment of £3,000 that covered the key features of these scams would have broken the spell and revealed the scam.

I say this because the scam Mr C fell victim to had a number of typical features of an investment scam that I would have expected to be mentioned in a relevant warning. For example, he found the investment on social media, and he was assigned a 'financial advisor' to help him with his trades and after some time a high value minimum amount was required for trades. These are key features of cryptocurrency investment scams that Mr C could have been clearly warned about.

Looking at the communication between Mr C and the scammer, I see no reason why a clear warning about the features of a cryptocurrency investment scam would not have broken the spell. I can't see that Mr C was so far under the spell of the scammer that he would have ignored a warning or sought guidance for the scammer on how to circumvent a warning.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr C 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 C might have been at risk of financial harm from fraud when they made the £3,000 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 C 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 C'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 C has only complained against Revolut. I accept that it's *possible* that other firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, and Mr C could instead, or in addition, have sought to complain against those firms. But Mr C 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 C'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 C's loss from the £3,000 Payment (subject to a deduction for Mr C's own contribution which I will consider below).

Should Mr C bear any responsibility for his losses?

I've finally considered whether or not Mr C should reasonably bear some responsibility for the losses as a result of any negligence in his actions and if it is therefore reasonable for me to make a reduction in the award based on this. In doing so, I've considered whether Mr C has acted as a reasonable person would to protect himself against the loss he suffered. The test is objective but needs to take account of the relevant circumstances.

In doing so, I have considered that Mr C initially thought it was his own daughter who had recommended the company in a post on social media. So, he felt the recommendation had come from a trusted source and I can therefore understand why he felt the investment was legitimate. He also says he carried out some research on the initial company, which did not have negative reviews. I can see that a short time later, there was some worrying information about the company online, however by that point Mr C's 'advisor' had let him know he was stepping away from the company and would be working with a new liquidity provider. So, I don't think Mr C would reasonably have had concerns the investment was not legitimate.

I can also see Mr C was told he would receive returns, but these did not appear to be too good to be true. Instead, they appeared to grow gradually over time and eventually Mr C was encouraged to make larger investments to get higher value returns respectively.

On balance, having carefully reviewed the evidence, I don't think Mr C acted unreasonably in the circumstances in a way that contributed to his loss. I therefore do not think a reduction in the redress is warranted in this particular case.

Putting things right

Redress

Revolut should reimburse Mr C from the payment of £3,000 onwards and also apply 8% simple interest to this amount from the date of the transactions to the date of settlement, and it can deduct any lawful tax from this.

My final decision

I uphold Mr C's complaint in part and recommend Revolut Ltd pay the redress outlined above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 28 May 2025.

Rebecca Norris
Ombudsman