

The complaint

Mr M complains that Revolut Ltd won't refund money he lost when he fell victim to an investment scam.

Mr M is being represented by solicitors in this complaint.

What happened

Mr M came across an investment firm, "C", on the internet. His representative states that Mr M invested a small amount (around £200) from his main bank before depositing a further £550 from his existing e-money account with Revolut as recommended by C. Following these payments, C cut contact with Mr M.

A few weeks later, Mr M was contacted by another company, "W", who offered to assist him in recovering his investment in return for a payment. Mr M allowed W remote access as requested. He states W obtained credit in his name through his main bank. These funds were then transferred to his Revolut account before being sent on to a cryptocurrency exchange for conversion into cryptocurrency. The cryptocurrency was then sent to crypto wallets.

Mr M states he was unaware of the credit being obtained and payments being made from his Revolut account. It was only when he checked his main bank account that he realised what had happened and discovered he had been scammed.

The following transactions, which took place from Mr M's Revolut account in January and February 2023, are relevant to this complaint –

	Date	Type	Payee	Amount
Payment 1	26 January	Debit card	Mr M's wallet with B	£16
Payment 2	31 January	Debit card	Mr M's wallet with B	£550
Payment 3	20 February	Debit card	Mr M's wallet with B	£10,000
Payment 4	21 February	Debit card	Mr M's wallet with B	£5,000
Payment 5	22 February	Debit card	Mr M's wallet with B	£7,000
Payment 6	22 February	Debit card	Mr M's wallet with B	£1,500
Payment 7	22 February	Debit card	Mr M's wallet with B	£710
			Total loss	£24,776

Revolut declined to refund any of the disputed payments, saying that Mr M had authorised them. It also said Mr M didn't do any due diligence before making them.

Our investigator was satisfied that Mr M knew about and consented to the disputed transactions and completed some of the steps involved. So, they were authorised. The investigator thought that the first two payments weren't unusual, but Revolut ought to have intervened and questioned Mr M when he authorised Payment 3. Had it done so, they were persuaded that the scam would have been uncovered and further losses prevented. They

asked Revolut to refund Mr M's losses from that payment onwards along with interest, but with a 50% deduction for contributory negligence.

Mr M eventually accepted the investigator's findings and recommendation, but Revolut didn't. In summary, it states it is irrational and illogical to hold Revolut liable in circumstances where it merely served as an intermediary in the transfers – the scam didn't occur on Revolut's platform. It also says that the Financial Ombudsman Service has irrationally failed to consider the fact that these transactions are self-to-self.

As an agreement couldn't be reached, the case has been passed to me to decide.

What I've decided – and why

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

In broad terms, the starting position at law is that an Electronic Money Institution ("EMI") such as Revolut is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

And, as the Supreme Court has recently reiterated in *Philipp v Barclays Bank UK PLC*, subject to some limited exceptions banks have a contractual duty to make payments in compliance with the customer's instructions.

In that case, the Supreme Court considered the nature and extent of the contractual duties owed by banks to their customers when making payments. Among other things, it said, in summary:

- The starting position is that it is an implied term of any current account contract that, where a customer has authorised and instructed a bank to make a payment, it must carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risk of its customer's payment decisions.
- At paragraph 114 of the judgment the court noted that express terms of the current account contract may modify or alter that position. In *Philipp*, the contract permitted Barclays not to follow its consumer's instructions where it reasonably believed the payment instruction was the result of APP fraud; but the court said having the right to decline to carry out an instruction was not the same as being under a legal duty to do so.

In this case, the terms of Revolut's contract with Mr M 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'm 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'm 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.

While 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 January 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'm 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 January 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'm 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.

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.

- 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 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 January 2023 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;

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

- 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.

While I'm required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I'm satisfied that to comply with the regulatory requirements that were in place in January 2023, Revolut should in any event have taken these steps.

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

It isn't in dispute that Mr M 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). The Financial Conduct Authority published a warning about C on 2 February 2023. And although there's no regulator warning about W (to my knowledge), from what Mr M has described about what happened and the text conversation and emails I've seen I'm satisfied that it's more likely than not that W was a scam company.

I'm aware that cryptocurrency exchanges generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. Revolut would likely have been aware of this fact too. So, it could have reasonably assumed that most of the disputed payments would be credited to a cryptocurrency wallet held in Mr M's name.

By January 2023, when these transactions started, 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.

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.

NatWest Group, Barclays, Lloyds Banking Group and Santander had all introduced some restrictions on specific cryptocurrency exchanges by August 2021.

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'm satisfied that by the end of 2022, prior to the payments Mr M made in January 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.

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 M'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 M might be at a heightened risk of fraud that merited its intervention.

I think Revolut should have identified that the payments were going to a cryptocurrency provider (the merchant involved is a well-known cryptocurrency provider). Payments 1 and 2 were low in value, and I don't think Revolut should reasonably have suspected that they might be part of a scam.

However, Payment 3 was significantly larger than any other payment Mr M had made from his Revolut account in the year leading up to it. Given what Revolut also knew about the destination of the payment, I think that the circumstances should have led it to consider that Miss M was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements, I'm 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 M?

Revolut didn't provide any warnings to Mr M before executing his authorised instructions in relation to any of the disputed payments.

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.

Having thought carefully about the risk Payment 3 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 M's account. I think it should have done this by, for example, directing Mr M to its in-app chat to discuss the payment further.

If Revolut had attempted to establish the circumstances surrounding Payment 3, would the scam have come to light and prevented the losses Mr M suffered from that point?

Had Mr M told Revolut that he was purchasing cryptocurrency because a company was assisting him in getting his money back, that they had contacted him about that unprompted, and that he had been asked to use remote access software so they could help him with it, Revolut would have immediately recognised that he was falling victim to a scam. It would have been able to provide a very clear warning that gave details about investment scams involving cryptocurrency and how he could protect himself from the risk of fraud.

I've reviewed the text conversation between Mr M and the scammer (though I note that he appears to have also spoken to them not just communicated by instant message, and I haven't heard those conversations). I've found nothing within those conversations that suggests Mr M was asked, or agreed to, disregard any warning provided by Revolut. I've also seen no indication that Mr M expressed mistrust of Revolut – with whom he had an account with since 2018 – or financial firms in general.

Given that Mr M had no desire to lose his money, it's very likely that he would have stopped, not followed the scammer's instructions and his loss would have been prevented from that point onwards.

Ultimately, as Revolut didn't question the payments Mr M made, it can provide no compelling evidence that he would have misled it about the purpose of the payments or the surrounding circumstances. Therefore, on the balance of probabilities, had Revolut provided Mr M with an impactful warning that gave details about cryptocurrency investment scams and how he could protect himself from the risk of fraud, I believe it would have resonated with him. I'm satisfied that a timely warning to Mr M from Revolut would very likely have caused him to decide not to go ahead with Payment 3.

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

In reaching my decision about what is fair and reasonable, I've taken into account that Mr M purchased cryptocurrency which credited an e-wallet held in his own name, rather than making a payment directly to the scammer. So, he remained in control of the money after he made the payments from his Revolut account, and it took further steps before the money was lost to the fraudsters.

I've carefully considered Revolut's view that in a multi-stage fraud, a complaint should be properly considered only against either the firm that is a) the 'point of loss' – the last point at which the money (or cryptocurrency) remains under the victim's control; or b) the origin of the funds – that is the account in which the funds were prior to the scam commencing. It says it is (in this case and others) merely an intermediate link – being neither the origin of the funds nor the point of loss and it is therefore irrational to hold it responsible for any loss. But as I've set out in some detail above, I think that Revolut still should have recognised that Mr M might have been at risk of financial harm from fraud when he made Payment 3, and in those circumstances it should have declined the payment and made further enquiries. If it had taken those steps, I'm satisfied it would have prevented the losses Mr M suffered. The fact that the money used to fund the scam came from elsewhere and/or wasn't lost at the point it was transferred to Mr M'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 M 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 M could instead, or in addition, have sought to complain against those firms. But he hasn't chosen to do that and ultimately, I can't 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 M'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'm satisfied that it would be fair to hold Revolut responsible for Mr M's loss from Payment 3 (subject to a deduction for his own contribution which I will consider below).

Should Mr M bear any responsibility for his losses?

I've thought about whether Mr M should bear any responsibility for his loss. In doing so, I've considered what the law says about contributory negligence, as well as what I consider to be fair and reasonable in all of the circumstances of this complaint.

Here, payments made from Payment 3 onwards were in relation to recovering money already sent. When asked what due diligence he carried out before deciding to deal with W, who had seemingly contacted him out of the blue, Mr M said he just took their word. Given that C, who he originally sent payments to, cut contact with him shortly after the payments, I consider it reasonable that Mr M ought to have been more cautious before deciding to part with even more money. Especially, when he was being asked to pay a lot more money than he'd originally invested – even if the refund included 'profits' on his investment. Based on the information I've seen, it would appear that an initial investment of less than £1,000 had grown to over £40,000 in a month. And Mr M was being asked to pay nearly half of that balance to recover it. I consider there were red signs here which ought to have given Mr M cause for concern.

Having carefully thought about this, I consider it would be fair for the reimbursement due to Mr M to be reduced because of his role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

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

Mr M sent money to a cryptocurrency provider before transferring it to the fraudster (albeit he didn't know that at the time). Revolut wouldn't have been able to recover the funds from the cryptocurrency provider, given that the funds had already been transferred out.

Putting things right

Revolut Ltd needs to refund 50% of the outstanding loss from and including Payment 3. I make that amount to be £12,105.

Revolut Ltd also needs to add simple interest at 8% per year to the individual refunded amounts, calculated from the date of loss to the date of settlement.

If Revolut considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Mr M how much it's taken off. It should also give Mr M a tax

deduction certificate if he asks for one, so he can reclaim the tax from HM Revenue & Customs if appropriate.

My final decision

For the reasons given, my final decision is that I uphold this complaint. Revolut Ltd needs to put things right for Mr M as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 6 December 2024.

Gagandeep Singh
Ombudsman