

The complaint

Ms C complains that Revolut Ltd won't refund money she lost when she fell victim to a scam.

What happened

Ms C saw an advert online for an investment opportunity with a company which I'll call T. She followed a link to what she thought was a professional looking website and left her details.

She was then contacted directly by a representative of T who helped her through setting up her trading account and advised her to download remote access software and to open a Revolut account to facilitate payments to cryptocurrency platforms. Unfortunately, and unknown to Ms C, T was not legitimate, she was dealing with a scammer.

Ms C made an initial small investment from another account, and when she saw that had performed well, she then made two much larger investments from her Revolut account. In total, Ms C made payments in Euros and in Sterling which totalled over £10,000. The relevant payments she made to the scam are detailed below.

Payment	Date	Amount	Payee
Payment 1	30/03/2023	£1,760	Card payment to crypto
Currency exchange	27/04/2023	£10,000	Converted to Euros
Payment 2	27/04/2023	€11,200	Transfer to crypto

Towards the end of the scam Ms C asked to withdraw her profits. She was told he'd need to pay more money to facilitate this withdrawal. When she refused, and was then denied access to her trading account, she realised she had been scammed.

Ms C contacted Revolut to let it know what had happened, but it declined to refund any of the disputed payments. Revolut said that it had intervened appropriately in the payments Ms C had made and that it could not have done more to prevent the scam.

Unhappy with this, Ms C referred her complaint to our service. Our Investigator felt Revolut could have done more to question Ms C about the second payment she made to the scam, and that it would have been able to prevent her loss from that payment if it had done so. So, they recommended that Revolut refund Ms C's loss from that second payment, with a deduction of 50% to recognise Ms C's contributory negligence to what happened.

Revolut did not accept the Investigator's findings. It said the payment was made to an account in Ms C's own name at the cryptocurrency platform, and so did not think it should be held liable for that loss. Revolut also questioned whether any other bank involved in the payment journey had intervened in the payments Ms C was making.

As an agreement couldn't be reached, the complaint 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 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 Ms C 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 Ms C and the Payment Services Regulations to carry out her 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

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

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 early 2023 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).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”*.
- 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

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/

³ 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.

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 Code⁴, 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, 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 early 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.

What did Revolut do to warn Ms C and what should it have done?

It isn't in dispute that Ms C fell victim to a cruel scam. Nor is it disputed that she authorised the payments which she now seeks reimbursement for.

The first payment that Ms C made to the scam, while it was identifiably to a cryptocurrency provider, was relatively low, so I think it was reasonable that Revolut did not intervene in this payment bearing in mind the limited risk it represented.

⁴ BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

But Revolut evidently then did identify that Ms C may be at risk of a scam, as on 31 March 2023 it contacted her in its in-app chat to ask some questions about her account. At this time, Ms C told Revolut that she had downloaded remote access software, and that she was being 'walked through possibilities of investing'. Revolut asked who was assisting her, but Ms C did not answer as she said she was busy at work. When the chat resumed a few days later Revolut asked what the nature of the payments she was making was and Ms C said she was wanting to make a transfer to her own account at a high-street bank. Revolut referred back to what Ms C had said about being guided to invest, and then provided some limited information about investment scams and asked Ms C some questions about what she was investing in. Ms C provided only limited answers to these questions. After providing another fairly generic warning about scams Revolut unblocked Ms C's account.

A few weeks later Ms C then tried to make the much larger second payment to the scam. Again, Revolut identified this as potentially suspicious, and asked Ms C what the payment was for. Ms C said it was to pay for goods or services, and then went through to the in-app chat to discuss the payment further. Revolut asked some closed questions about whether Ms C had been contacted unexpectedly and told to move her money, and provided warnings relating to safe account scams and purchase scams before unblocking the account and allowing the payment to go ahead.

Revolut says Ms C should have selected 'investment' which was an available option when she was prompted for a payment purpose. But regardless of what option Ms C should have selected, Revolut ought to have been concerned given the circumstances of this payment. Specifically, that it was aware Ms C had recently been trying to invest in cryptocurrency, that she had told it she was being guided in that investment, and that she had said she had downloaded remote access software (a significant hallmark of many scams). And bearing this in mind, along with the high value of the payment being made, and that it was a foreign currency transaction to a payee associated with cryptocurrency, I don't consider displaying a scam warning, was a proportionate response to the risk identified.

Having thought carefully about the risk the transaction presented, I think a proportionate response to that risk would be for Revolut to have attempted to establish the detailed circumstances surrounding the transaction before allowing it to debit Ms C's account. I think it should have done this by asking some open questions about what Ms C was doing and what the payment was for, and satisfying itself that this was for a legitimate purpose before allowing the payment to go ahead.

If Revolut had taken this action, would that have prevented the losses Ms C suffered?

I've considered this point carefully. I've not seen anything to suggest that Ms C was given any cover story to use regarding the payments she was making. And it is clear that she was open and honest about what the payments were for in the early stages of the scam. So, I consider it very likely that, had Revolut asked her at the time of payment 2, Ms C would have again been open and honest about what she was making the payment for – transferring her money to a cryptocurrency account for the purposes of an investment. I appreciate that Ms C did not select the 'investment' payment purpose when asked what the payment was for, but I don't consider that this was necessarily an attempt at deception. And I consider that there were several features of the scam which would have been easily brought to light by some direct questioning, and which would have rung significant alarm bells for Revolut.

For example, Ms C had been asked to download remote access software by the scammers, had found the investment via an online advert, and was being guided in how to invest. These are very common features of this kind of cryptocurrency investment scam, and Revolut would have been aware of such scams at the time of the payment. I think this would have

been enough to put Revolut on notice that Ms C was at risk of falling victim to a scam, and a reasonable action at that stage would have been to provide a more detailed scam warning relevant to cryptocurrency investment and to explain how these red flags indicated that the investment was likely not legitimate and what Ms C could do to check the legitimacy of what she believed she was investing in. I've seen nothing to make me think that Ms C would have ignored such a direct warning.

I'm aware that Ms C had seen a warning about investment scams earlier on in the scam, but that warning had contained limited detail about how she could protect herself or what to look out for. And at the time she saw it she was trying to make a payment to her own bank account, not a payment associated with the investment, so I can see why it would not have resonated with her at that time.

With all this in mind, I think that it would have been possible for Revolut to identify that Ms C was the victim of a scam and to provide her with an appropriate warning at the time of payment 2 that would have resonated with her and so prevented her from making this payment.

I'm aware that Ms C moved some funds from an account she held with another bank into her Revolut account to fund the scam. But that other bank did not intervene in the payments Ms C made. So, at the time I think Revolut should have intervened, Ms C had not seen (or ignored) any detailed warnings regarding what he was doing. With this in mind, I think it's fair to say that, had Revolut intervened appropriately, then it is likely that the spell of the scam would have been broken, and that Ms C wouldn't have proceeded with the payment. So, I think Revolut could have prevented the losses Ms C incurred from payment 2.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Ms C moved some funds into her Revolut account from another UK bank, and that the payments she made out of her Revolut account were to a cryptocurrency account in her own name that she had access to.

But as I've set out above, I think that Revolut still should have recognised that Ms C might have been at risk of financial harm from fraud when she made payment 2, and in those circumstances Revolut should have made further enquiries about the payment before processing it. If it had done that, I am satisfied it would have prevented the losses Ms 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 Ms C's crypto account does not alter that fact and I think Revolut can fairly be held responsible for Ms C's 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 Ms C has only complained against Revolut. I accept that it's *possible* that other firms might also have missed the opportunity to intervene – although I've seen nothing to suggest that those firms did intervene – or failed to act fairly and reasonably in some other way, and Ms C could instead, or in addition, have sought to complain against those firms. But Ms C has not chosen to do that and ultimately, I cannot compel her to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Ms 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 Ms C's loss from payment 2 (subject to a deduction for Ms C's own contribution which I will consider below).

Should Ms C bear any responsibility for her losses?

There's a general principle that consumers must take responsibility for their decisions. I've duly considered whether Ms C should bear some responsibility by way of contributory negligence. And considering the details of this scam I do think it is fair that she bear some responsibility for her losses.

Ms C has accepted that she should also bear some responsibility here, so I won't go into this point in any great detail. But, in summary, I think there were aspects of the way Ms C found the investment and how it progressed that should have given her cause for concern about what she was doing.

So, having thought carefully about this, I do think that Ms C ought to bear some responsibility for her losses and that the refund due to her should be reduced by 50% accordingly.

I've also thought about whether Revolut did all it could to try to recover Ms C's funds when she told it of the scam. But bearing in mind the delay in the scam being reported, and that the payments made were to purchase cryptocurrency, I don't consider that there was anything more that Revolut could have done to recover Ms C's funds.

Putting things right

To resolve this complaint Revolut Ltd should now:

- Refund 50% of Ms C's loss from payment 2; and
- Pay 8% simple interest per annum on the refunded amount, calculated from the date of payment 2 to the date of settlement (less any tax properly deductible).

My final decision

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

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms C to accept or reject my decision before 19 June 2025.

Sophie Mitchell
Ombudsman