

The complaint

Mr O complains that Revolut Ltd (“Revolut”) didn’t do enough to protect him when he fell victim to a scam.

What happened

The details of this complaint are well known to both parties, so I won’t repeat them again here. Instead, I’ll summarise what happened and focus on giving the reasons for my decision.

Between May and June 2023, Mr O made payments to a cryptocurrency exchange totalling just over £15,000 to what he believed was a legitimate investment. But he realised he’d been the victim of a scam following an attempt to make a withdrawal, after which his balance started to decrease at an alarming rate.

Our investigator considered this complaint. He concluded that Revolut should have intervened at the time of the second payment (of six) which was for £3,018 by way of a tailored written warning. He thinks this intervention would have unravelled the scam. And he didn’t think Mr O should bear any responsibility for the loss.

Mr O agreed but Revolut didn’t. In summary, it said the funds were transferred to Mr O’s own account with a third party, that the payments being made weren’t out of character or unexpected, and that other bank’s may have intervened so this should be considered too.

So, 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.

Having done so, I agree with the outcome reached by our investigator – I’m upholding this complaint from the second payment onwards. I’ll explain why below.

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 O 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 May 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 May 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 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

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”

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

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

It isn't in dispute that Mr O has fallen victim to a cruel scam here, nor that he authorised the card payments to a cryptocurrency exchange (from where that cryptocurrency was subsequently transferred to the scammer).

I don't think Revolut would have had any reason to intervene with the first payment made to the cryptocurrency exchange – for £1,000. But by May and June 2023, when these transactions took place, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency for some time. I think Revolut should have identified the risk of financial harm at the point of payment two. This payment was for £3,018, was clearly going to a cryptocurrency provider and brought the total spend that day to cryptocurrency to £4,018. Mr O hadn't made payments that were identifiably to cryptocurrency, nor had he made payments as high as this in value, in the preceding months.

Given what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Mr O 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.

To be clear, I do not suggest that Revolut should provide a warning for every payment made to cryptocurrency. Instead, as I've explained, I think it was a combination of the characteristics of this payment (combined with those which came before it, and the fact the payment went to a cryptocurrency provider) which ought to have prompted a warning.

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 O attempted to make the second payment, knowing that the payment was going to a cryptocurrency provider, to have provided a warning 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 O 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 O suffered from the second payment?

I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case. And on the balance of probabilities, I think it would have. There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Mr O's payments, such as being assisted by an agent and being asked to download remote access software.

I've also reviewed the conversation between Mr O and the fraudsters (though I note that Mr O appears to have spoken to the fraudster over the telephone, not just communicated by instant message, and I haven't heard those conversations). I've found nothing within those conversations that suggests Mr O was asked, or agreed to, disregard any warning provided by Revolut. I've also seen no indication that Mr O expressed mistrust of Revolut or financial firms in general. Neither do I think that the conversation demonstrates a closeness of relationship that Revolut would have found difficult to counter through a warning.

The evidence I've seen persuades me that Mr O was not so taken in by the fraudsters that he wouldn't have listened to the advice of Revolut. We've also been advised by the firms from which funds used for the scam originated from that either no warning was provided, or low-level warnings were provided.

Therefore, on the balance of probabilities, had Revolut provided Mr O 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 O from Revolut would very likely have revealed the scam and prevented his further losses.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr O purchased cryptocurrency which credited an e-wallet held in his own name, rather than making a payment directly to the fraudsters. So, it took further steps before the money was lost to the fraudsters.

But as I've set out above, I think that Revolut still should have recognised that Mr O might have been at risk of financial harm from fraud when they made the second 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 O 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 O's own account does not alter that fact and I think Revolut can fairly be held responsible for consumer'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 Mr O 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 O has not chosen to do that and ultimately, I cannot compel them to. In those circumstances, I can only make an award against Revolut. I'm also not persuaded it would be fair to reduce Mr O'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 O's loss from the second payment.

Should Mr O bear any responsibility for his losses?

I've also thought about Mr O's part in his own losses here. In doing so, I've taken into account what the law says about contributory negligence, while keeping in mind that I need to decide this case based on what I consider to be fair and reasonable in all the circumstances.

Having done so, I don't think the evidence supports that Mr O should bear responsibility for his losses. Mr O found the purported investment when looking online for opportunities so wasn't contacted out of the blue. Having reviewed the communication with the scammer, I've seen no mention of the specific returns Mr O would be receiving, so there's nothing here to suggest they were unrealistic. Rather, he started investing and appears to have been led to believe the investment was doing well.

I've seen a contract that Mr O was required to sign and, though there was mention of a risk-free trade which would generally be considered too good to be true, this was said to be valid on the first trade only and for a limited period, making it come across as more realistic. Mr O had carried out searches on the company involved in the investment but didn't find anything overly concerning. And, while there's now an FCA warning about the company, this was first published after Mr O had made all of his payments.

On that basis, I don't think it would be fair to hold Mr O liable for his losses.

Putting things right

So, in order to put things right for Mr O, Revolut Ltd must:

- Reimburse Mr O from (and including) payment two onwards;
- Pay 8% simple interest per annum on this amount from the dates of payment to the date of settlement.

My final decision

For the reasons given, I uphold this complaint against Revolut Ltd and direct it to put things right as set out above within 28 days of acceptance of this decision.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr O to accept or reject my decision before 8 April 2025.

Melanie Roberts
Ombudsman