

## **The complaint**

Mr C complains that Revolut Ltd hasn't protected him from losing money to an investment scam.

## **What happened**

The background to this complaint is well known to both parties, so I won't repeat everything here. In brief summary, Mr C has explained that from February to June 2023 he made 13 card payments from his Revolut account for what he thought was a legitimate investment. The payments (including associated fees) totalled £33,923.54 plus €5,000.

Mr C subsequently realised he'd been scammed and got in touch with Revolut. Ultimately, Revolut didn't reimburse Mr C's lost funds, and Mr C referred his complaint about Revolut to us. As our Investigator couldn't resolve the matter informally, the case has been passed to me for a decision.

I sent Mr C and Revolut my provisional decision on 25 February 2025. Now both parties have had fair opportunity to respond, I'm ready to explain my 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.

Mr C told us that he accepts my provisional decision. And Revolut didn't respond to my provisional decision. So, in the absence of evidence or arguments persuading me otherwise, I've reached the same conclusions as in my provisional decision, and for the same reasons. I've explained my reasons again 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 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 in February to June 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;<sup>1</sup>
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;

---

<sup>1</sup> 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/](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/)

- using the confirmation of payee system for authorised push payments;
- providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified.

For example, it is my understanding that in February to June 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)<sup>2</sup>.
- 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 Code<sup>3</sup>, 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 –

---

<sup>2</sup> 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.

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

particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

- The main card networks, Visa and Mastercard, don't allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain restrictions on their card issuers' right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of transaction, such as by location. The network rules did not, however, prevent card issuers from declining particular payment instructions from a customer, based on a perceived risk of fraud that arose from that customer's pattern of usage. So it was open to Revolut to decline card payments where it suspected fraud, as indeed Revolut does in practice (see above).

Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in February to June 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.

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

It isn't in dispute that Mr C has fallen victim to a scam here, nor that he authorised the payments he made to the cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammers).

I'm aware that cryptocurrency exchanges like the one Mr C paid 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 these payments would be credited to a cryptocurrency wallet held in Mr C's name.

By February to 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. 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<sup>4</sup>. And during the period of February to June 2023, when these payments took place, further restrictions were in place<sup>5</sup>. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

I recognise that, as a result of the actions of other payment service providers, many customers who wish to purchase cryptocurrency for legitimate purposes will be more likely to use the services of an EMI, such as Revolut. And I'm also mindful that a significant majority of cryptocurrency purchases made using a Revolut account will be legitimate and not related to any kind of fraud (as Revolut has told our service). However, our service has also seen numerous examples of consumers being directed by fraudsters to use Revolut accounts in order to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider, a fact that Revolut is aware of.

So, taking into account all of the above, I am satisfied that by the end of 2022, prior to the payments Mr C made in February to June 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

To be clear, it is the specific risk associated with cryptocurrency in February to June 2023 that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm.

In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice, and to comply with regulatory requirements, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. And as I have explained, Revolut was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact the payments in this case were going to an account held in Mr C's 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. And I think that Revolut should have identified that Mr C's first payment of £3,000 on 27 February 2023 was going to a cryptocurrency provider and – given

---

<sup>4</sup> 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.

<sup>5</sup> In March 2023, both Nationwide and HSBC introduced similar restrictions to those introduced by Santander in November 2022.

the amount it was for and what I've said about the rise in cryptocurrency scams – recognised Mr C was at heightened risk of financial harm from fraud, such that it was appropriate for it to intervene proportionately and warn him.

What did Revolut do to warn Mr C?

It's my understanding that Revolut has said that Mr C had to authorise these card payments through the 3DS system but that, when this was done, it didn't intervene in the payments or warn Mr C about the possibility he was falling victim to a 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 instructed this first payment, knowing the payment was going to a cryptocurrency provider, to have provided, at a minimum, a warning (whether automated or in some other form) that was specifically about the risks of cryptocurrency scams, given how prevalent they had become by the end of 2022.

I think 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 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. 'Fees' becoming payable to initiate withdrawals that then don't fully materialise or are restricted or small in value would also be a common theme.

I recognise that a warning of this 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.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr C suffered from this first payment onwards?

I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented the losses 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 C's payments, such as an advertisement on social media, promoted by a celebrity or public figure; an 'account manager', 'broker' or 'trader' acting on their behalf; and the use of remote access software.

I've also reviewed the available evidence of contact between Mr C and the fraudsters and I've found nothing to suggest Mr C would have disregarded any warnings provided by Revolut. I appreciate Revolut has made reference to an email it says it sent Mr C in May 2023. But I agree with what our Investigator has said about this. Not only was this largely too late, but I've not seen evidence Mr C actually saw that email, nor do I think this would be as

impactful as an in-app warning adding significant friction to the payments at the actual time Mr C was instructing them.

I've also seen no other evidence that satisfies me Mr C wouldn't have taken any tailored warnings from Revolut at the actual time of the payments on board, had Revolut provided them as I've said it should have.

Therefore, on the balance of probabilities, had Revolut provided Mr C 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. He could have paused and looked more closely into the 'broker' or 'platform' before proceeding further, as well as making further enquiries into cryptocurrency scams and whether or not the broker was regulated in the UK or abroad. And in this case, there was an FCA warning published on 9 February 2023 about the outfit Mr C thought he was dealing with. And bearing this in mind, as well as other information Mr C would likely have discovered about scams like this, I think it's most likely that had Revolut done what it should have done, Mr C most likely would have paused and then ultimately not have proceeded to make and lose these payments from his Revolut account to the scam.

#### 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 some of the funds that Mr C paid from his Revolut account to the crypto exchange (which were then sent on from there to the scammers) were funded by money from his account with a third party bank "Bank C".

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 he made his first 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/or 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 Mr 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 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 first payment onwards (subject to a deduction for Mr C's own contribution which I will consider below).

### Should Mr C bear any responsibility for his losses?

In considering this point, I've taken into account what the law says about contributory negligence, as well as what's fair and reasonable in the circumstances of this complaint. And here I think it is fair to say Mr C wasn't as careful with his payments as he reasonably ought to have been.

I note in this regard that Mr C's representative has said that Mr C first came across the scammers in January 2023 and that was when Mr C looked into the opportunity, so he wouldn't have seen, for example, the warning the FCA published about them on 9 February 2023. I've taken on board everything Mr C's representative has said about this. However, I can see from the communications exchanged between Mr C and the scammers that on 14 February 2023 (before Mr C made the first of his payments from his Revolut account on 27 February 2023) Mr C was informed by the scammers that their website was changing; Mr C was advised of a further change to the website in April 2023. This ought to have been concerning. Mr C also borrowed considerable funds in order to make the majority of these payments to the scam. And given the circumstances of the payments, their amounts, and Mr C's position and what the scammers were telling him, I think he ought to have been concerned and looked into things further such that I think it is fair that Mr C bears responsibility for half of the total loss.

### Recovery

For completeness, I'll address recovery. After these payments were made, because they were debit card payments, the only potential avenue to recover them would have been through the chargeback scheme. However, Mr C didn't make the debit card payments to the scammers. Instead, he made them to a legitimate crypto exchange, which would have provided the services intended. So Revolut could only have brought chargeback claims against the crypto exchange (and not the scammers) but these wouldn't have succeeded given the circumstances. So I can't say Revolut unreasonably hindered recovery of the funds.

### Putting things right

Our Investigator explained in his assessment that the available information suggests that of the funds lost to the scam, £10,400 originated from Mr C's account with Bank C, and that Mr C borrowed the rest from other people who paid it directly into his account with Revolut before Mr C sent it on to exchange it for cryptocurrency. I understand Mr C still owes this money to the people he borrowed it from. But whilst he's suffered that loss, he hasn't suffered a loss from the loss of the use of that money since, because he wouldn't have borrowed it but for the scam. So there is no need for Revolut to pay Mr C compensatory interest apart from on the amount he lost from his own resources – which is £10,400. However, as I've said Mr C should bear responsibility for half of it, I'm satisfied fair compensatory interest is for Revolut to pay Mr C interest calculated at 8% simple on the amount of £5,200 only.

Our Investigator explained in his assessment the difficulties of choosing a precise date for when that interest should be paid from. And I agree with his recommendation that 28 March 2023 represents a fair date bearing the details of the various payments in mind. He also explained why it would be appropriate for the one payment made out of Mr C's account in EUR to be refunded by way of an equivalent amount of GBP calculated using the exchange rate of the time it was exchanged which was on 27 March 2023.



## **My final decision**

For the reasons explained, I uphold this complaint in part and I direct Revolut Ltd to pay Mr C:

- £16,961.77; plus
- an equivalent amount to €2,500 as GBP – at the exchange rate of the time it was exchanged which was on 27 March 2023.
- interest on the amount of £5,200 calculated at 8% simple per year from 28 March 2023 to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 9 April 2025.

Neil Bridge  
**Ombudsman**