

The complaint

Mr C is unhappy that Revolut Ltd won't reimburse him funds lost after he was a victim of fraud.

What happened

As the circumstances of this complaint are well-known to both parties, I have summarised them briefly below.

In July 2023, Mr C received an unsolicited telephone call regarding an investment opportunity involving cryptocurrency (crypto).

Mr C registered his interest and was passed over to a contact within the purported firm. But, unbeknown to Mr C at the time, he was in fact speaking with a person intent on defrauding him.

In August 2023, Mr C was persuaded to make an initial payment to a crypto platform where his funds were converted to digital assets and sent on to the fraudster. He was also given access to an online platform where he could see the progress of his investment, which appeared to be performing well.

Mr C says that this persuaded him to invest more, and, between August and December 2023, he made further payments to the crypto platform from his Revolut account. He also, on two occasions, converted fiat currency to crypto using his Revolut account and sent that on to the fraudsters.

For ease, a full list of the payments is as follows:

Payment number and date	Amount	Type of transaction
1. 14 August 2023	£862	Card payment
2. 29 August 2023	£3,442	Card payment
3. 4 September 2023	£2,138	Card payment
4. 14 September 2023	£1,300	Conversion to crypto
5. 25 September 2023	£1,431.38	Card payment
6. 5 December 2023	£750	Conversion to crypto

Mr C eventually realised he'd been the victim of a fraud when he'd paid money to release his funds, but they weren't. So he reported the matter to Revolut.

Revolut looked into Mr C's claim, but it didn't agree it had made an error. So Mr C brought

his complaint to our service for an independent review.

An Investigator considered the complaint and found Revolut ought to have done more to protect Mr C from the second payment he'd made. But they also found Mr C should hold equal liability for his loss. They therefore recommended a 50% refund from that payment.

Revolut disagreed with the Investigator's findings and recommendations, so the matter has now been passed to me for a final decision to be made.

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 Mr 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 Mr C and the Payment Services Regulations to carry out their 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 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 August 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).
- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the *“Financial crime: a guide for firms”*.
- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut’s obligation to monitor its customer’s accounts and scrutinise transactions.

¹ 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 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/>

- 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).
- Since 31 July 2023, under the FCA's Consumer Duty⁴, regulated firms (like Revolut) must act to deliver good outcomes for customers (Principle 12) and must avoid causing foreseeable harm to retail customers (PRIN 2A.2.8R). Avoiding foreseeable harm includes ensuring all aspects of the design, terms, marketing, sale of and support for its products avoid causing foreseeable harm (PRIN 2A.2.10G). One example of foreseeable harm given by the FCA in its final non-handbook guidance on the application of the duty was *"consumers becoming victims to scams relating to their financial products for example, due to a firm's inadequate systems to detect/prevent scams or inadequate processes to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers"*⁵.
- 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 August 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;
- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;
- 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

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

⁴ Prior to the Consumer Duty, FCA regulated firms were required to "pay due regard to the interests of its customers and treat them fairly." (FCA Principle for Businesses 6). As from 31 July 2023 the Consumer Duty applies to all open products and services.

⁵ The Consumer Duty Finalised Guidance FG 22/5 (Paragraph 5.23)

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 cruel fraud here, nor that he authorised the payments made to his crypto wallet (from where that crypto was subsequently transferred to the fraudster).

Whilst I have set out in this decision the circumstances which led Mr C to make the payments using his Revolut account and the process by which that money ultimately fell into the hands of the fraudster, I am mindful that, at that time, Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Mr C might be the victim of fraud.

Firstly, I don't find that Revolut had any reason to intervene in the first payment Mr C made. While it was a larger payment than he tended to make from the account, it wasn't so large that it fell significantly outside of the normal operation of the account.

However, the second payment made to the crypto platform stood out. It was significantly higher than any payment Mr C had made in the preceding year and was out of character when considering the way Mr C normally spent on his account.

Furthermore, by August 2023, when these transactions took place, firms like Revolut had been aware of the risk of multi-stage frauds involving cryptocurrency for some time. Fraud involving cryptocurrency had increased over time. The FCA and Action Fraud published warnings about cryptocurrency fraud in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency fraud have continued to increase since. They reached record levels in 2022.

So, taking the above into account, I am satisfied that by the end of 2022, prior to the payment Mr C made in August 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.

The second payment made was clearly going to a crypto provider and was significantly out of character for the account. I find that this ought to have flagged to Revolut that there was a credible risk to Mr C when he was attempting to make this payment. And so it follows that Revolut ought reasonably to have intervened in that payment.

What did Revolut do to warn Mr C?

Revolut has confirmed it didn't intervene in the payment(s) made. Nor did it present Mr C with any warnings.

What kind of warning should Revolut have provided?

The FCA's Consumer Duty, which was in force at the time these payments were made, requires firms to act to deliver good outcomes for consumers including acting to avoid foreseeable harm. In practice this includes maintaining adequate systems to detect and prevent fraud and to design, test, tailor and monitor the effectiveness of fraud warning messages presented to customers.

I'm mindful that firms like Revolut have had warnings in place for some time. It, along with other firms, has developed those warnings to recognise both the importance of identifying the specific fraud risk in a payment journey and of ensuring that consumers interact with the warning.

In light of the above, I think that by August 2023, when the second payment took place, Revolut should have had systems in place to identify, as far as possible, the actual fraud that might be taking place and to provide tailored, effective warnings relevant to that fraud for both APP and card payments.

In this case, Revolut knew that the second payment was being made to a cryptocurrency provider, and its systems ought to have factored that information into the warning it gave.

There is no reason to believe Mr C wouldn't have been honest regarding the reason he was making the payment. And considering the prevalence of crypto investment scams, I'd have expected Revolut to have provided this as an option for why the customer was making the payment.

This ought to have prompted Revolut to deliver a warning that highlighted the common features of such frauds, and the risks associated with them.

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

The features associated with the fraud Mr C was victim to were common.

He'd received unsolicited contact, was provided access to an online platform that showed his investment had grown exponentially, and it appears the fraudsters used the name of a genuine, FCA authorised firm to add weight to their legitimacy: commonly referred to as cloning.

Also important here is that prior to Mr C carrying out the second transaction, he was sent a document informing him that he had to make a further payment of €4,000 to lift restrictions on his account and withdraw his funds: a very common feature of investment fraud.

Had Revolut pointed out to Mr C the features commonly associated with these types of fraud, it's likely this would have resonated with him as they were relevant to his circumstances. I find it likely this would have uncovered the fraud and prevented Mr C from continuing with any further payments to the fraudster.

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 consideration that Mr C's Revolut account was sometimes a conduit between Mr C paying money from one of his bank accounts to his crypto wallet.

But as I've set out 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 the second payment. 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 Mr C suffered. The fact that the money used to fund the fraud came from elsewhere, and wasn't lost at the point it was transferred to Mr C's own crypto wallet, 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 payment two onwards (subject to a deduction for Mr C's own contribution which I will consider below).

Revolut has addressed an Administrative Court judgment, which was referred to in a decision on a separate complaint. As I have not referred to or relied on that judgment in reaching my conclusion in relation to the losses for which I consider it fair and reasonable to hold Revolut responsible, I do not intend to comment on it.

I note that Revolut says that it has not asked me to analyse how damages would be apportioned in a hypothetical civil action but, rather, it is asking me to consider all of the facts of the case before me when considering what is fair and reasonable, including the role of all the other financial institutions involved.

I have considered the role of the other financial institution involved in the payment journey when thinking about how Mr C may have reacted to warnings that Revolut ought to have provided. But as no warnings were given by the third-party bank, this has not altered my findings. The third-party bank has also confirmed that Mr C has not been reimbursed any of the payments made from that account.

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.

Mr C has provided minimal evidence pertaining to the original agreement he'd entered into with the fraudster. Many of the documents provided are in relation to the latter release of funds requests or messages between both parties that have not been translated to English.

However, even without this information, I am satisfied that there were sufficient red flags present here that ought to alerted Mr C to a potential risk.

I acknowledge that Mr C was an inexperienced investor, so he likely didn't hold sufficient knowledge regarding the specific investment he was embarking on which would allow him to fully protect himself. But even without this knowledge, there were things he ought to have been alerted to, or acted upon, that he did not.

Mr C was cold called by the fraudster – something that reasonably ought to heighten suspicions. Mr C was therefore unable to verify who they were. I accept that fraudsters can be persuasive once they've been given the opportunity to pitch their purported opportunity,

but Mr C ought to have been alive to the fact that he'd been contacted by a stranger and without any enquiry from his end first. While Mr C did check the company name on the official register, he'd not verified if the person he was talking to was a legitimate representative of that company.

Mr C was also guaranteed profits that ought to have raised suspicions. Had Mr C delved into these claims further, it's likely that he not only would have seen that they were well above what was realistically achievable, but that profits from trading cannot be guaranteed due to fluctuating markets.

Mr C has also provided evidence that at an early stage of the fraud (prior to the second payment he made) he was told to begin making payments to lift restrictions on his account and withdraw his funds. This letter claimed that he was guaranteed a withdrawal of €15,250.80: a profit he'd allegedly earned from an £862 initial investment. As well as the unrealistic claims regarding his returns, the letters do not sufficiently explain why Mr C was required to make the payments requested. I realise Mr C likely felt helpless in having to make the payment to recover the funds he'd already paid to the fraudster, but he also ought to have questioned the farfetched claims being made.

Overall, while I understand the persuasive tactics used by fraudsters involved in such crimes, I do find that Mr C ought to have better protected himself by heeding some of the warnings that were apparent in this fraud. As such, I find it reasonable that Mr C be equally liable for his loss here.

Recovery of funds and compensation

As neither party disagrees on these points—as they haven't contested the Investigator's findings on each—I don't intend to address these points in detail. However, I concur with the Investigator's assessment that:

1. The funds would not have been recoverable, as they were used to be converted into digital assets and sent on to the fraudster.
2. The distress and inconvenience caused here can predominantly be attributed to the person who defrauded Mr C, not Revolut.

Putting things right

Revolut should now reimburse Mr C 50% of the payments made to the fraudster from payment two, including the consequential losses of the crypto exchanges and their fees.

As it could have stopped these payments from the date they were made, it should apply 8% simple annual interest from those dates to the date it settles.

My final decision

For the reasons I've given above, I uphold this complaint and direct Revolut Ltd to:

- Reimburse Mr C 50% of the five transactions made from payment two.
- Pay 8% simple annual interest from the date each of the transactions were made to the date it settles.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 17 June 2025.

Stephen Westlake
Ombudsman