

The complaint

Mr B complains that Revolut Ltd won't refund payments he made as a result of a scam.

What happened

Mr B was the victim of an investment scam involving the following payments from his newly opened Revolut account:

Ref.	Date	Description	Amount
1	28 March 2023	Card Payment to 'Crypto.com' a cryptocurrency exchange	£4,978.75
2	31 March 2023	Card Payment to Simplex, a cryptocurrency exchange	£3,000.00
3	15 June 2023	Card Payment to Simplex	£2,010.00
4	19 June 2023	Card Payment to Simplex	£2,000.00
5	22 June 2023	Card Payment to Simplex	£2,000.00
6	26 June 2023	Card Payment to Simplex	£2,100.00
7	27 June 2023	Card Payment to Simplex	£2,200.00
8	3 July 2023	Card Payment to Simplex	£2,300.00
9	29 July 2023	Card payment to Moonpay, a cryptocurrency exchange.	£1,666.00

In summary, Mr B saw an advert for an investment opportunity on social media that appeared to be promoted by a prominent individual. After registering his details, he was contacted by one of N's account managers, who I'll call S.

Mr B initially made a card payment for £250.00 from another bank account to invest on N's trading platform. After seeing a profit, he invested more significant amounts in March 2023. To do this, he was instructed via remote access software to send money using a new Revolut account to a cryptocurrency exchange. From there, it was exchanged to crypto and sent to a wallet address S gave him. Mr B was tricked into thinking this deposited the funds on his account with N's online trading platform. In fact, the investment and platform were fake, and the funds credited fraudsters' wallets.

Believing he'd made money, Mr B attempted to make a withdrawal in June 2023, but he was told by a company I'll call 'B' that he'd need to pay to access the money – to cover, for example, supposed fees and fluctuations in the value of his investment. Having paid this and not heard, Mr B became concerned it was fraud and reported what happened to Revolut via its in-app chat facility in mid-July 2023. Revolut replied to say that because he confirmed the payments via its app, it couldn't consider them fraudulent.

Mr B subsequently heard from B that they'd send the money straight to his bank account, as the transfer to his crypto wallet supposedly wasn't working – and that he'd need to pay money to complete this successfully. After doing this, he didn't hear from the fraudsters again.

In October 2023, Mr B raised a complaint to Revolut, via professional representatives, that it

ought to have done more to protect him from the scam. Revolut didn't uphold it – in summary, it explained why it couldn't recover the payments he'd made via a chargeback claim.

Unhappy with its response, Mr B brought his concerns to us to investigate. I issued my provisional findings which upheld the complaint in part. Mr B accepted what I said, and Revolut didn't have anything further to add. So the complaint has come back to me to make a 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.

Given that neither side has added anything further in response to my provisional findings, I see no reason to change my mind. For completeness, I've included these findings 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 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.

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 March 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 EMIs 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 March 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.

¹ For example, Revolut's website explains it launched an automated anti-fraud system in August 2018: https://www.revolut.com/news/revolut_unveils_new_fleet_of_machine_learning_technology_that_has_seen_a_fourfold_reduction_in_card_fraud_and_had_offers_from_banks/

² Since 31 July 2023 under the FCA's new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.

- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of *“Financial crime: a guide for firms”*.
- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut’s obligation to monitor its customer’s accounts and scrutinise transactions.
- The October 2017, BSI Code³, which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).
- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer’s control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer’s own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.
- The main card networks, Visa and Mastercard, don’t allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain restrictions on their card issuers’ right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of transaction, such as by location. The network rules did not, however, prevent card issuers from declining particular payment instructions from a customer, based on a perceived risk of fraud that arose from that customer’s pattern of usage. So it was open to Revolut to decline card payments where it suspected fraud, as indeed Revolut does in practice (see above).

Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in March 2023 that Revolut should:

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

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

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

Whilst I have set the detailed circumstances which led Mr B to make the payments from his Revolut account and how that money ultimately fell into fraudsters' hands, I am mindful that, at that time, Revolut had much less information available to it to decide whether any of the payments presented an increased risk that Mr B might be the victim of a scam.

I'm aware that many cryptocurrency exchanges 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 would be credited to a cryptocurrency wallet held in Mr B's name.

By March 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.

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 us). 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 B made in March 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, I'm not suggesting as Revolut argues that, as a general principle (under the Consumer Duty or otherwise), Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees. As I've set out in some detail above, it is the specific risk associated with cryptocurrency in March 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 likelihood of the payments going to an account held in Mr B's own name should have led Revolut to believe there wasn't a risk of fraud.

So I've gone onto consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Mr B might be at a heightened risk of fraud that merited its intervention.

I'm satisfied Revolut should have identified that the first payment was going to a cryptocurrency provider (the merchant is a well-known cryptocurrency provider). I realise this was a new account, so Revolut didn't have a transaction history to say what usual expenditure looked like for Mr B. But that also means they couldn't have anything to say this wasn't *unusual*. I note that when he opened the account, he said it was 'transfers', rather than cryptocurrency. Moreover, I consider that this was a reasonably significant single payment – for just under £5,000.00.

Coupled with what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Mr B was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements, I am 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 which ought to have prompted a warning.

Revolut argues that it is unlike high street banks in that it provides cryptocurrency services in

addition to its electronic money services. It says that asking it to 'throttle' or apply significant friction to cryptocurrency transactions made through third-party cryptocurrency platforms might amount to anti-competitive behaviour by restricting the choice of its customers to use competitors. As I have explained, I do not suggest that Revolut should apply significant friction to every payment its customers make to cryptocurrency providers. However, for the reasons I've set out above I'm satisfied that by March 2023 Revolut should have recognised at a general level that its customers could be at increased risk of fraud when using its services to purchase cryptocurrency and, therefore, it should have taken appropriate measures to counter that risk to help protect its customers from financial harm from fraud. Such proportionate measures would not ultimately prevent consumers from making payments for legitimate purposes.

What did Revolut do to warn consumer, and what kind of warning should it have provided?

Revolut didn't warn Mr B when he made these card payments. So I've gone on to consider 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 B attempted to make the first payment, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form) 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 scams, 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 B 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 consumer suffered?

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 B's complaint, such as finding the investment through an advertisement endorsed by a public figure, being assisted by an account manager, and being asked to download remote access software.

I've also reviewed the text conversation between Mr B and the fraudsters (though I note that

Mr B appears to have spoken to the fraudster, not just communicated by instant message, and I haven't heard those conversations). I've not found anything within those conversations that persuaded me that Mr B was asked, or agreed to, disregard any warning provided by Revolut.

I've noted that Mr B did seem reliant on S's help using the cryptocurrency exchanges. But I don't think there's enough to conclude that he was being shown relevant scam warnings as part of this, and that S was persuading him to ignore them. I've also seen no evidence that Mr B was provided with warnings by the firm used to top up his Revolut account.

I've taken into account that Mr B made a payment after suggesting he'd been defrauded to Revolut as he'd not heard from S – and I've considered whether that means even if he'd been warned, he'd have carried on regardless. But having reviewed his conversation with the Revolut agent, I note that they didn't educate him about investment scams – they only checked he made the payments and said they couldn't consider them fraudulent. So it was never made clear to Mr B that he had, in fact, been scammed. I'm also mindful that, by this point, Mr B appeared desperate to get his money back, given what he'd invested. Taking this all into account, I don't think it's enough to say that a clear warning, provided earlier on, wouldn't have changed his mind.

Therefore, on the balance of probabilities, had Revolut provided Mr B 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 before proceeding, as well as making further enquiries into cryptocurrency scams and whether or not the broker was regulated in the UK or abroad. I'm satisfied that a timely warning to Mr B from Revolut would very likely have caused him to take the steps he did take – revealing the scam and preventing his 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 B purchased cryptocurrency which credited an e-wallet held in his own name, rather than making a payment directly to the fraudsters. So, he remained in control of his money after he made the payments from his Revolut account, and it took further steps before the money was lost to the fraudsters.

I have carefully considered Revolut's view that in a multi-stage fraud, a complaint should be properly considered only against either the firm that is a) the 'point of loss' – the last point at which the money (or cryptocurrency) remains under the victim's control; or b) the origin of the funds – that is the account in which the funds were prior to the scam commencing. It says it is (in this case and others) merely an intermediate link – being neither the origin of the funds nor the point of loss and it is therefore irrational to hold it responsible for any loss.

In reaching my decision, I have considered that the payments were made to another financial business (a cryptocurrency exchange) and that the payments that funded the scam were made from another account at a regulated financial business.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr B might have been at risk of financial harm from fraud when he made the 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 B 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 his own account does not alter that fact and I think Revolut can fairly be held responsible for his loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

I've also considered that Mr B 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 he 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 B's compensation in circumstances where: he 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 consumer's loss from the first payment (subject to a deduction for Mr B's own contribution which I will consider below).

Should Mr B bear any responsibility for their 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.

I can see how Mr B, who had seemingly little investment experience, was taken in by the scam. It was advertised on social media, seemingly promoted by a prominent individual that many trust on money matters. And from the screenshots Mr B shared, N's platform looked professional and sophisticated, and he'd access to his own account and account manager.

Mr B's representatives said he saw reviews online via a popular website before he invested. But I've noted these didn't appear until after he made the first payment towards the scam at the beginning of March 2023 (via his other account). In any event, I accept that, had Mr B carried out research online before he invested, there was little available to discredit N.

I've also noted how Mr B initially invested a relatively small amount. And it wasn't until he saw supposed profits from his investment that he sent more significant amounts. And generally, while S suggested money could be made from the investment, I've not seen he was offered significant and guaranteed profits, in a manner that looked too good to be true.

I've also noted that S was not overly pushy – and they didn't pressure Mr B to repeatedly invest in a way that might arouse suspicion. Instead, after he invested in March, no further payments were sent until June, which was to withdraw the money.

While I've highlighted aspects of the scam that made it convincing, I find there were causes for concern as the scam continued. Mr B was repeatedly asked to pay varying amounts to withdraw what he earned. While I appreciate how, as an inexperienced investor, Mr B was duped by the technical descriptions of why they needed to be paid, I think he ought to have become more suspicious sooner about the repeated demands for payment. Particularly as he ended up paying more to access what he had earned than he had originally invested. And especially as he made a payment after he'd clearly concerns it was a scam.

Taking this all into account, I've reduced some of the award to reflect Mr B's contributory negligence. I consider that while Revolut should refund all of Mr B's losses from payments 1 to 4, it should only refund 50% of his losses from Payments 5 to 9, which was the third payment that was supposedly in connection with his withdrawal from N.

My final decision

For the reasons I've explained, I uphold Mr B's complaint. Revolut Ltd must pay Mr B:

- the total of his losses from payments 1 to 4
- the total of his losses from payments 5 to 9, minus 50% to reflect his contributory negligence
- 8% simple interest per year on this amount, from the dates of the payments to the date of settlement (less any tax lawfully deductible).

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 19 August 2025.

Emma Szkolar
Ombudsman