

## The complaint

Mrs B complains that Revolut Ltd won't refund money she lost when she fell victim to an investment scam.

Mrs B is being represented by solicitors in this complaint.

## What happened

Mrs B says that in or around June 2023, when she was researching how to make extra money, her family told her about a company "X" they had come across online and had since spoken to. X had advised them not to invest given their circumstances. Mrs B decided to contact X and find out more about the investment opportunity.

Shortly after leaving her contact details on X's website, Mrs B was contacted by an individual who claimed to be a representative. They talked her through the cryptocurrency investment opportunity and Mrs B decided to open an account with X. She started with an initial deposit of \$250 which she sent from her account held with her main bank. On seeing her increased profits, and to take advantage of a time sensitive opportunity, Mrs B was persuaded to make further deposits.

Under the instructions of her 'account manager', Mrs B opened an e-money account with Revolut to facilitate the deposits. She first transferred funds from her bank account to her e-money account with Revolut. The money was then used to purchase cryptocurrency from cryptocurrency providers, before being sent to cryptocurrency wallets as instructed by her account manager. At the time, Mrs B believed the cryptocurrency was being deposited into her account with X as its balance went up by the same amount. The use of remote access software was involved.

When Mrs B subsequently asked to make a withdrawal, she was told this needed to be arranged through a different firm. That firm advised her that she hadn't traded for long enough and therefore needed to make a payment totalling 50% of what she had already paid to 'prove liquidity'. It was at this point that Mrs B realised she had fallen victim to a scam.

The following transactions are relevant to this complaint –

	Date	Type	Payee/details	Amount
Payment 1	8 June 18:19	Debit card	Cryptocurrency provider 1	£1,999
Payment 2	8 June 18:53	Debit card	Cryptocurrency provider 2	£2,600
			<b>Total loss</b>	<b>£4,599</b>

Revolut declined to refund any of the disputed payments, saying that Mrs B had authorised them.

Unhappy with this, Mrs B referred her complaint to our service through her representative. Our investigator ultimately thought that the first payment wasn't unusual, but Revolut ought to have provided a warning specific to cryptocurrency scams when Mrs B authorised

Payment 2. Had it done so, the investigator was persuaded that the scam would have been uncovered and further losses prevented. They asked Revolut to refund Mrs B's losses from that last payment along with interest, but with a 50% deduction for contributory negligence.

Mrs B accepted the investigator's outcome, but Revolut didn't. It provided an 18-point reply which set out why it disagreed with the investigator's view and the general approach our service takes on these types of cases.

As the matter couldn't be resolved informally, Mrs B's case has been passed to me to decide.

### **What I've decided – and why**

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

In 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 Mrs B 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'm 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'm 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.

While 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 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'm 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;<sup>1</sup>
- 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 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'm 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>.

---

<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/)

<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.

- 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 – 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 June 2023 that Revolut should:

---

<sup>3</sup> 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.

While I'm required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I'm satisfied that to comply with the regulatory requirements that were in place in June 2023, Revolut should in any event have taken these steps.

*Should Revolut have recognised that Mrs B was at risk of financial harm from fraud?*

It isn't in dispute that Mrs B has fallen victim to a cruel scam here, nor that she authorised the payments she made to her cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

I'm aware that cryptocurrency exchanges 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 most of the disputed payments would be credited to a cryptocurrency wallet held in Mrs B's name.

By June 2023, when these transactions happened, 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 by 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

---

<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.

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'm satisfied that by the end of 2022, prior to the payments Mrs B made in 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.

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 most of the payments in this case were going to an account held in Mrs B's own 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 Mrs B might be at a heightened risk of fraud that merited its intervention.

I think Revolut should have identified that both payments were going to a cryptocurrency provider (the merchants involved are well-known cryptocurrency providers). Payment 1 was low in value, and I don't think Revolut should reasonably have suspected that it might be part of a scam. However, Payment 2 was relatively larger, and it was made within 40 minutes of the previous payment.

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

#### What did Revolut do to warn Mrs B?

Revolut didn't provide any warnings to Mrs B before executing her authorised instruction to make Payment 2.

#### 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 Mrs B attempted to make Payment 2, 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 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 Mrs 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 Mrs B suffered from Payment 2?*

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 Mrs B’s payments, such as being assisted by a broker and being asked to download remote access software so they could help her.

I’ve also reviewed the text conversation between Mrs B and the fraudsters (though I note that Mrs B appears to have also spoken to the fraudster, not just communicated by instant message, and I haven’t heard those conversations). I’ve found nothing within those conversations that suggests Mrs B was asked, or agreed to, disregard any warning provided by Revolut. I’ve also seen no indication that Mrs B expressed mistrust of Revolut or financial firms in general.

Therefore, on the balance of probabilities, had Revolut provided Mrs B with an impactful warning that gave details about cryptocurrency investment scams and how she could protect herself from the risk of fraud, I believe it would have resonated with her. She could have, for instance, 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 Mrs B from Revolut would very likely have caused her to decide not to go ahead with Payment 2.

*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’ve taken into account that Mrs B purchased cryptocurrency which credited an e-wallet held in her own name, rather than making a payment directly to the fraudsters. So, she remained in control of her money after she made the payments from her Revolut account, and it took further steps before the money was lost to the fraudsters.

I’ve 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.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mrs B might have been at risk of financial harm from fraud when they made Payment 2, and in those circumstances it should have declined the payment and made further enquiries. If it had taken those steps, I'm satisfied it would have prevented the losses Mrs B 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 Mrs B's own account does not alter that fact and I think Revolut can fairly be held responsible for her 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 Mrs 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 Mrs B could instead, or in addition, have sought to complain against those firms. But she hasn't chosen to do that and ultimately, I can't compel her to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mrs B'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'm satisfied that it would be fair to hold Revolut responsible for consumer's loss from Payment 2 (subject to a deduction for Mrs B's own contribution which I will consider below).

#### *Should Mrs B bear any responsibility for her losses?*

Mrs B has accepted that she should share equal responsibility for her losses from Payment 2, as per our investigator's outcome. For completeness, I'll address why I'm in agreement that liability should be shared equally between the parties.

There's a general principle in law that consumers must take responsibility for their decisions. I recognise that there were relatively sophisticated aspects to this scam, not least an apparently credible and professional looking platform. I also understand that Mrs B checked X's reviews which she says were largely positive.

But, as the investigator highlighted (and I agree), there were several negative reviews about X at the time of Mrs B's payments. In fact, a scam warning about it was published by the FCA in 2020. A link to that warning came up on the first page of the results when I've done a backdated search on X on the internet.

Having thought carefully about this, I'm in agreement with the investigator that Mrs B ought to bear some responsibility for her losses because of her role in what happened, and that compensation should be reduced accordingly. Weighing up everything, I consider that it would be fair to reduce compensation payable by 50%. As I've mentioned, Mrs B accepts this.



### Could Revolut have done anything to recover Mrs B's money?

Mrs B sent money to a cryptocurrency provider before transferring it to the fraudster (albeit she didn't know that at the time). Revolut wouldn't have been able to recover the funds from the cryptocurrency provider, given that the funds had already been transferred out.

### **Putting things right**

Revolut Ltd needs to refund Payment 2, making a 50% deduction for contributory negligence.

Revolut Ltd also needs to add simple interest at 8% per year to the refunded amount, calculated from the date of loss to the date of settlement<sup>6</sup>.

### **My final decision**

For the reasons given, my final decision is that I uphold this complaint. I require Revolut Ltd to put things right for Mrs B as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs B to accept or reject my decision before 21 November 2024.

Gagandeep Singh  
**Ombudsman**

---

<sup>6 6</sup> If Revolut considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Mrs B how much it's taken off. It should also give Mrs B a tax deduction certificate if she asks for one, so she can reclaim the tax from HM Revenue & Customs if appropriate.