

The complaint

Mrs B complains that Revolut Ltd won't refund money she lost when she was the victim of a scam.

A representative who I will call "C" complains on behalf of Mrs B.

What happened

The background to this complaint is well known to both parties, so I won't repeat it in detail here. But in summary and based on everything sent by both parties, I understand it to be as follows.

Between April and July 2023, Mrs B lost a total of £23,970.54 when she made eight payments to what she thought was a legitimate cryptocurrency investment she had seen advertised online. Unfortunately, Mrs B realised the investment was actually a scam when, after paying withdrawal fees, she still didn't receive her funds.

A table showing all of the payments made in relation to the fraud is set out below.

Date and Time	Amount	Description	Type
2023-04-04 14:49:22	1,000.00 GBP	Payment to crypto	Card payment
2023-04-13 10:44:23	1,000.00 GBP	Payment to crypto	Card payment
2023-05-29 11:17:21	5,000.00 GBP	Payment to crypto	Card payment
2023-05-29 12:37:28	2,608.47 GBP	Payment to crypto	Card payment
2023-05-29 12:53:21	383.00 GBP	Payment to crypto	Card payment
2023-07-26 12:59:33	5,000.00 GBP	Payment to crypto	Card payment
2023-07-26 16:51:47	3,700.00 EUR (£5,785.82)	Transfer to new payee	transfer
2023-07-27 10:56:53	6,704.00 EUR (£3,193.25)	Transfer to new payee	transfer

Revolut said they authorised the payments in line with Mrs B's instruction. They said they provided warnings for the payments, but Mrs B proceeded to make them. While they tried to recover the money they weren't able to, and overall said they weren't liable for the loss.

C referred Mrs B's complaint to our service on her behalf. Our investigator was of the opinion that Revolut was responsible for some of Mrs B's loss. He said Revolut should have been concerned when the first £5,000 payment was made as it was significantly higher than the previous transactions, out of character for the account, and was a large sum being paid to a cryptocurrency exchange.

He said the warnings Revolut did present were in relation to scams involving new payees, but as Revolut could see the money was being sent to a cryptocurrency provider, they should have shown warnings tailored to the risks associated with cryptocurrency investment scams. And had they done this, he thought it would've resonated with Mrs B – because of the similarities – and prevented her loss.

Our investigator thought Mrs B should also be responsible for her loss, and recommended Revolut refund 50% from the first £5,000 payment onwards. He also recommended Revolut pay 8% simple interest from the date of the payments to the date of settlement.

Revolut disagreed. They said the payments were self to self, meaning Mrs B owned the account they were made to. As a result, they said the fraud didn't occur on Mrs B's Revolut account as she only lost control of the funds when they left her crypto account. They also said the transactions were not out of character for how a typical EMI account is used. And they argued that it is relevant to consider other bank's interventions – such as the where the funds originated from – and whether that bank provided warnings to Mrs B. Because Revolut disagreed, the complaint was passed to me for 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.

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 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 were required by the terms of their 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 they suspected customers 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 April 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;
- 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.

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.
- The October 2017, BSI Code, 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 April 2023 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Revolut sometimes does); and
- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

Whilst I am required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I am satisfied that to comply with the regulatory requirements that were in place when the payments were made, 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 by transfers to third parties and to her cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

Whilst I have set out in detail in this decision the circumstances which led Mrs B to make the payments using her 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 them upon which to determine whether any of the payments presented an increased risk that Mrs B might be the victim of a scam.

I'm aware that cryptocurrency exchanges, like the one Mrs B used here, generally say that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder, along with the account used to receive payments from the exchange. Revolut would likely have been aware of this fact too. So, they could have reasonably assumed that the payments would be credited to a cryptocurrency wallet held in Mrs B's name.

By April 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. And by April 2023, when these payments took place, further restrictions were in place. 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 are aware of.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mrs B made from April 2023 onwards, Revolut ought fairly and reasonably to have recognised that their customers could be at an increased risk of fraud when using their 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 that as a general principle, 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 April 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 they processed such payments. And as I have explained Revolut were also required by the terms of their contract to refuse or delay payments where regulatory requirements meant they 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 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, they ought to have identified that Mrs B might be at a heightened risk of fraud that required their intervention.

The first two payments, which Revolut should've identified as going to a cryptocurrency provider, were of a low value and spread out. And so, I wouldn't reasonably have expected Revolut to have been concerned that Mrs B was at risk of financial harm from fraud at this point. But I think by the point of the third transaction (£5,000), the risk of potential financial harm from fraud had increased. This is because the value of the payment was much greater than those that preceded it, it was being made to a cryptocurrency provider which carries a

known fraud risk and being made on a relatively newly opened account (which can be a potential indicator of 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 Mrs B before this payment went ahead. To be clear, I do not suggest that Revolut should provide a warning for every payment made to cryptocurrency. Instead, as I've explained, I think it was a combination of the characteristics of this payment (combined with those which came before it, and the fact the payment went to a cryptocurrency provider) which ought to have prompted a warning.

What did Revolut do to warn Mrs B?

I haven't seen anything to show Revolut provided Mrs B with any scam warnings before processing this payment (or those that preceded it).

I am aware that Revolut did provide warnings to Mrs B before processing the last two payments (which were fund transfers). But the warnings provided were tailored to the payment purpose of "goods and services" that Mrs B selected. Because of this, the warnings Mrs B received weren't tailored to the risks and common features of cryptocurrency investment scams – and so, wouldn't have resonated with her.

In any event, given Revolut ought to have identified the card payments were being made to a crypto provider, I don't think the steps they took to protect Mrs B were sufficient. I think Revolut ought to have done more before processing the £5,000 payment on 29 May 2023.

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 full consideration to Revolut's primary 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 the £5,000 Payment, knowing (or strongly suspecting) that it was going to a cryptocurrency provider, to have provided a warning that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every 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 the first £5,000 payment onwards?

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 finding the investment through an advertisement endorsed by a popular television show, the scammer asking her to download remote access software on her device, a broker trading on her behalf and quick profits received from an initial small deposit.

I've also reviewed the text conversation between Mrs B and the fraudsters (though I note that Mrs B appears to have spoken to the fraudster on the phone too). I haven't found anything within the conversations that suggests Mrs B was asked, or agreed to, disregard any warnings provided by Revolut.

Nor have I seen that Mrs B ignored any warnings relevant to her situation – as her external bank provider, which funded these payments, weren't able to show that they interacted or provided any scam warnings during this time.

I've also seen no indication that Mrs B expressed mistrust of Revolut or financial firms in general. Neither do I think that the conversation demonstrates a closeness of relationship that Revolut would have found difficult to counter through a warning. I understand Mrs B did not agree to the fraudster's demands for her to pay fees to withdraw and it was this difficulty in withdrawing money that led her to uncover the scam.

Overall, the weight of evidence that I've outlined persuades me that Mrs B was not so under the spell of the fraudsters that she wouldn't have listened to the advice of Revolut. Because of this, and on balance, I think it's more likely than not that Mrs B wouldn't have made the third payment – or those that followed – had Revolut intervened as I would've expected.

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 paused and looked more closely into the investment before proceeding, as well as making further enquiries into cryptocurrency scams.

I'm satisfied that a timely warning to Mrs B from Revolut would most likely have revealed the scam, preventing her further losses.

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

In reaching my decision, I have taken into account that for some of the payments, Mrs B purchased cryptocurrency which credited an account 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.

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 she made the first payment of £5,000, and in those circumstances they should have declined the payment and made further enquiries.

If they had taken those steps, I am satisfied they would have prevented the losses Mrs 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 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 about Revolut. I accept that it's *possible* that the 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 them. But Mrs B has not chosen to do that and ultimately, I cannot 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 she has only complained about one respondent from which she is entitled to recover her 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 Mrs B's loss from the first £5,000 payment (subject to a deduction for Mrs B's own contribution which I will consider below).

Should Mrs B bear any responsibility for her 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 recognise that, as a lay person who claims to have little investment experience, there were aspects to the scam that would have appeared convincing. Mrs B was introduced to it through an online advert, where it looked to be endorsed by a popular television programme. Those adverts can be very convincing – often linking to what appears to be a trusted and familiar news source.

I can also understand how what might have seemed like taking a chance with a smaller sum of money snowballed into losing a very large amount of money. So I've taken all of that into account when deciding whether it would be fair for the reimbursement due to Mrs B to be reduced. Having done so, I think it should.

Mrs B said she carried out some research before investing and saw positive reviews. But having checked myself, I can see there were several negative reviews from that time. And I think it would've been reasonable for Mrs B to have found these reviews as part of her checks (as they were prominent search results). So, I think these reviews should've put Mrs B on notice that there was a risk that the investment opportunity may not be genuine. I find it reasonable that she should have therefore been more cautious – such as seeking advice from others, whether they be her existing bank, friends, internet searches on crypto or seeking independent financial advice.

I also think Mrs B should have recognised the return offers were unrealistic, there was no formal contract in place, and most of the communication was done via instant messenger or on social media and over the phone. I think these things should, despite the investment appearing somewhat professional, have put her on notice that the investment might not be genuine.

Given everything, I've concluded on balance, that Revolut can fairly reduce the amount it pays to Mrs B because of her role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

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

I've also thought about whether Revolut could have done more to recover the funds after Mrs B reported the fraud.

The card payments were made to a legitimate crypto exchange to purchase cryptocurrency. And so, I'm not persuaded there would have been any reasonable prospect for a chargeback claim succeeding, as the merchant would be able to demonstrate that it had provided the goods/services that had been purchased using the card (in this case, the cryptocurrency that was then sent on to the scammer). So I don't think there was anything more Revolut could've done to recover the money in these circumstances.

In relation to the two transfers made, I can see that Revolut contacted the beneficiary to see whether there were any funds remaining in the account. Unfortunately, the money had been removed on the same day the payments were made (before the disputed payments were reported). Because of this, Revolut wasn't able to recover any of the funds lost.

Overall, for the reasons I've explained, I consider that Revolut should be liable for 50% of the funds lost from the first £5,000 payment onwards. I think it should also pay 8% simple interest to recognise the loss of use of money Mrs B suffered.

My final decision

My final decision is that I uphold this complaint in part. Revolut Ltd should pay Mrs B:

- 50% of the transactions from 29 May 2023 onwards. A total of £10,985.27.
- 8% simple interest per year from the date of each payment to the date of settlement.
-

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs B to accept or reject my decision before 21 August 2025.

Danielle Padden
Ombudsman