

The complaint

Mrs T complains that Revolut Ltd won't refund money she lost to a scam.

What happened

Mrs T said the following transactions were made as a result of a cryptocurrency investment scam.

Payment	Date	Type of transaction	Amount
1	2 February 2023	Debit card payment	£701.71
2	8 February 2023	Debit card payment	£4,000.00
3	13 February 2023	Debit card payment	£3,061.44
4	23 February 2023	Faster payment	£100.00
5	23 February 2023	Debit card payment	£5,000.00
	24 February 2023	Credit	£100.00
6	26 February 2023	Debit card payment	£5,000.00
7	27 February 2023	Debit card payment	£5,000.00
8	28 February 2023	Debit card payment	£5,000.00
9	1 March 2023	Debit card payment	£4,000.00
10	15 March 2023	Faster payment	£2.00
	15 March 2023	Credit	£170.00
11	21 March 2023	Faster payment	£100.00
12	27 March 2023	Faster payment	£40,000.00
	3 April 2023	Credit	£857.32
	11 April 2023	Credit	£721.22
13	19 April 2023	Faster payment	£10,000.00
	5 May 2023	Credit	£1,264.50

15	29 June 2023	Faster payment	£7,000.00
16	6 July 2023	Faster payment	£8,000.00

In summary, Mrs T said she came across an article online regarding a cryptocurrency investment opportunity and contacted the third party. Under the guidance of the scammer, Mrs T opened accounts on several cryptocurrency platforms and an account with Revolut.

After making several payments, Mrs T said she realised she had been scammed when she could no longer access the portal to see what she believed were her trades and she was unable to get in contact with the scammer. Mrs T contacted Revolut, but it didn't refund the money she lost.

Mrs T brought her complaint to our service and our investigator upheld it. He thought Revolut should have recognised that Mrs T might have been at heightened risk of harm from fraud when she made the 8th payment and had it intervened, it could have prevented the scam. However, he also thought Mrs T should bear some liability for her losses.

Revolut didn't accept what our investigator said and as an agreement couldn't be reached, the complaint 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.

I have considered all the available evidence 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 T modified the starting position described in *Philipp*, by – among other things – expressly requiring Revolut to refuse or delay a payment “*if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks*” (section 20).

So Revolut was required by the terms of its contract to refuse payments in certain circumstances, including to comply with regulatory requirements such as the Financial Conduct Authority's Principle for Businesses 6, which required financial services firms to pay due regard to the interests of their customers and treat them fairly. I am satisfied that paying due regard to the interests of its customers and treating them fairly meant Revolut should have been on the look-out for the possibility of fraud and refused card payments in some circumstances to carry out further checks.

In practice Revolut did in some instances refuse or delay payments at the time where it suspected its customer might be at risk of falling victim to a scam.

I must also take into account that the basis on which I am required to decide complaints is broader than the simple application of contractual terms and the regulatory requirements referenced in those contractual terms. I must determine the complaint by reference to what is, in my opinion, fair and reasonable in all the circumstances of the case (DISP 3.6.1R) taking into account the considerations set out at DISP 3.6.4R.

Whilst the relevant regulations and law (including the law of contract) are both things I must take into account in deciding this complaint, I'm also obliged to take into account regulator's guidance and standards, relevant codes of practice and, where appropriate, what I consider to have been good industry practice at the relevant time: see DISP 3.6.4R. So, in addition to taking into account the legal position created by Revolut's standard contractual terms, I also must have regard to these other matters in reaching my decision.

Looking at what is fair and reasonable on the basis set out at DISP 3.6.4R, I consider that Revolut should in February 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;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 February 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and

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/

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.
- 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 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

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.

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

straight away whether to accept or refuse the payment. They also place certain restrictions on their card issuers' right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of transaction, such as by location. The network rules did not, however, prevent card issuers from declining particular payment instructions from a customer, based on a perceived risk of fraud that arose from that customer's pattern of usage. So it was open to Revolut to decline card payments where it suspected fraud, as indeed Revolut does in practice (see above).

Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in February 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 in February 2023, Revolut should in any event have taken these steps.

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

By February 2023, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency (that is scams involving funds passing through more than one account controlled by the customer before being passed to a fraudster) 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 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 January 2023, when these payments took place, further restrictions were in place. 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 the vast 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.

So, taking into account all of the above, I am satisfied that, by the end of 2022, prior to the payments Mrs T made in February 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. In those circumstances, as a matter of what I consider to have been fair and reasonable and good practice, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments.

Taking the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact the payments in this case were going to an account held in Mrs T's own name and that the account opening reasons Mrs T gave included cryptocurrency should have led Revolut to believe there wasn't a risk of fraud.

I accept that the account was newly opened therefore Revolut did not have information on Mrs T's usual account activity that it could use to identify whether the payments were unusual for her. Nevertheless, Revolut did have information about the payments themselves which it ought to have taken into consideration.

What did Revolut do to warn Mrs T and what should it have done?

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.

I find Revolut should have intervened when Mrs T attempted to make payment 2, and 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.

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 think it would have been a proportionate way for Revolut to minimise the risk of financial harm to Mrs T by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

But I've also thought about whether a warning of this nature would have had a positive impact on Mrs T and caused her to stop and investigate further. I don't think it would, and I say this because Revolut intervened when Mrs T attempted to make payment 4 which was a faster payment to a new payee. It's shown that when asked, Mrs T stated the purpose of the payment as cryptocurrency. Revolut said Mrs T was then shown a tailored warning relevant to the scam risk associated with cryptocurrency related transactions.

The warning Mrs T would have seen when making payment 4 did, as described above, cover the key features of a cryptocurrency scam. Including a warning about downloading screen sharing software which Mrs T had done. Despite this, Mrs T proceeded with the payment. I don't find the circumstances between payment 2 and payment 4 to have been different, therefore I think it's unlikely Mrs T would have taken heed to the warning if it had been provided earlier.

However, I find Revolut had further opportunities to intervene, specifically, I think it ought to have intervened when Mrs T made payment 8, this is because the frequency of payments had increased, with Mrs T making payments of £5,000 in three days, consecutively. Taking into consideration the value of payment 8, and that by this time Mrs T had already made payments of close to £20,000 within a few weeks, the bulk of which was made in under a week, and were all identifiably related to cryptocurrency. I think a proportionate response to the risk at this time would be for Revolut to have attempted to establish the circumstances surrounding the payment before allowing it to debit Mrs T's account. I think it should have done this by, for example, directing Mrs T to its in-app chat to discuss the payment further with a member of staff.

I've thought about whether Mrs T would have been honest if questioned about the payment's purpose and I think she would. I say this because Mrs T gave accurate information when Revolut intervened in payment 4. She was honest about the account purpose when she opened it, and I can't see that she had been coached or provided with a cover story to give Revolut if it questioned her.

Had Mrs T informed Revolut that she had found the investment opportunity online, she had been asked to download screen sharing software, told to set up several accounts with cryptocurrency providers and told she could double her money in a few weeks, I think Revolut would have been able to recognise she was falling victim to a scam. It would have then been able to give a clear warning that legitimate investment firms do not make use of screen sharing software to carry out trading, and the returns she had been promised appeared to be too good to be true. It could have encouraged Mrs T not to make any further payments and to carry out research.

I appreciate that Mrs T proceeded with payment 4 despite being shown an automated warning. Mrs T said she didn't recall seeing the warning, so I think it's clear she did not give the information she was presented attention. But on balance, I think it's likely that if stopped and asked to discuss the payment, Mrs T would have reacted positively to the warnings provided by a member of staff. Considering that the money represented a significant amount of her and her husband's savings and was set aside to provide for them in retirement. At the very least, I think a warning would have prompted Mrs T to investigate further, by carrying out her own research into the firm and the broker. Revolut could have also informed Mrs T that the lack of information available online regarding the investment firm should in itself be a red flag.

Is it fair and reasonable for Revolut to be held responsible for Mrs T's loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Mrs T made the payments to an account in her own name rather than directly to the fraudsters.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mrs T might have been at risk of financial harm from fraud when she made Payment 8, and in those circumstances, it should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it could have prevented the losses Mrs T 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 T's own account does not alter that fact and I think Revolut can fairly be held responsible for Mrs T's loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

I've also considered that Mrs T 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 T could instead, or in addition, have sought to complain against those firms. Nevertheless, she 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 T's compensation in circumstances where: the consumer has only complained about one respondent from which they are entitled to recover their losses in full; has not complained against the other firm (and so is unlikely to recover any amounts apportioned to that firm); and where it is appropriate to hold a business such as Revolut responsible (that could have prevented the loss and is responsible for failing to do so). That isn't, to my mind, wrong in law or irrational but reflects the facts of the case and my view of the fair and reasonable position.

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be referred to me) and for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Mrs T's loss from Payment 8 (subject to a deduction for Mrs T's own contribution which I will consider below).

Should Mrs T bear any responsibility for her losses?

I accept that there were aspects of the scam that were sophisticated and would have appeared genuine to Mrs T. For instance, Mrs T said the scammer sounded knowledgeable and she was directed to download an investment platform, which she has provided evidence of, and I can understand why she might have thought it to be legitimate.

However, I find there were aspects of the scam that were questionable. Mrs T said she was told she could double her money in a few weeks, and that her money would always be safe, and I think this ought to have raised some questions that the returns might be too good to be true.

Mrs T said that when she was instructed to open an account with Revolut she was told that it would be easier "as the traditional banks did not like their customers investing due to the profits to be made rather than monies sitting in a savings account earning little to no interest." I think this ought to have made Mrs T question whether the scammer was genuine.

Mrs T said she did not do any research into the investment opportunity. Considering the amount of money she was looking to invest; I would expect some research to have been carried out here. Mrs T said she was told the company was UK based and had several offices around the country, however I find no evidence of the investment or the broker when carrying out a search online. So I think that had she carried out her own research, the lack of information would have caused Mrs T to pause.

I understand that Mrs T fell victim to a sophisticated scam, and whilst I sympathise with her and the situation she found herself in, I don't think she acted reasonably for the reasons I've given. As such, I find Mrs T ought to bear equal responsibility for the loss from payment 8 onwards.

Did Revolut do enough to recover Mrs T's money?

Mrs T made some payments via her debit card to the cryptocurrency platforms. The only means of recovery for these payments is through the Chargeback scheme. There are specific rules under which a claim can be made under the scheme. As the payments were made to a legitimate cryptocurrency exchange platform and to an account in Mrs T's name, a claim was unlikely to succeed.

Revolut said it attempted to recover the faster payments Mrs T made, but unfortunately it wasn't able to. Where payments are made because of fraud, we usually find the scammers quickly move the funds, usually within the first 24 hours, from the recipient account. As Mrs T reported the scam several months after the payments had been made, I find there were no real prospects of recovering the funds.

My final decision

For the reasons I've set out above, I uphold this complaint and require Revolut Ltd to:

- Deduct the £1,748.54 Mrs T received and then refund 50% of what remains from Payment 8 to Payment 16 (not including payment 15 which I address below)
- It should apply 8% simple interest, per year, for loss of use of her money during this time - calculated from the date of each payment to the date of settlement.
- Mrs T borrowed money from a friend to fund the investment and has provided evidence to show the loan was repaid in April 2024. Therefore, it should refund 50% of Payment 15 and pay 8% simple interest from the date the loan was repaid until the date of settlement.

If Revolut Ltd considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Mrs T how much it's taken off. It should also give Mrs T a tax deduction certificate if she asks for one, so she can reclaim the tax from HM Revenue & Customs if appropriate.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs T to accept or reject my decision before 25 April 2025.

Oluwatobi Balogun
Ombudsman