

The complaint

Mrs B complains that Revolut Ltd did not refund a series of payments she lost to a scam.

What happened

Mrs B was contacted via a messaging app about an investment opportunity, which turned out to be a scam. She was told the investment was buying and selling currencies and she started with a deposit of £99.25. On the platform, which turned out to be fake, she could see she was earning around 10% returns on her investment, and was convinced to invest more.

Eventually, she ran out of funds to invest but the scammer convinced her to take out a loan, and told her she would be able to pay it back in just three months with the profits. She therefore took out a loan with a third-party bank on 9 May 2023, and then sent another £30,000 to the investment over the next few days. However, she was told an error had occurred and the balance on her investment platform went to below zero. She was told that she needed to deposit £8,000 to balance the account again, so she did so with funds she borrowed from a friend. Mrs B made the following payments from her Revolut account:

Date	Amount	Type
15/04/2023	£99.25	CARD
29/04/2023	£1,000	CARD
04/05/2023	£1,000	CARD
09/05/2023	£21,000	TRANSFER
11/05/2023	£5,000	CARD
13/05/2023	£4,000	CARD
13/05/2023	£5,000	CARD
17/05/2023	£1,000	CARD
18/05/2023	£7,000	CARD

When she went to withdraw her profits, she was told she would need to take out a safety deposit box with a bank and would need to pay £9,000 for this. Mrs B spoke with her friend again who warned her something did not sound right. After going to the police, Mrs B realised she had been the victim of a scam and contacted Revolut to raise a scam claim.

Revolut issued a final response letter in which they explained Mrs B had made card payments to a legitimate company, and she had not requested a chargeback so they did not think they could do more to help her in the circumstances. Mrs B referred the complaint to our service and our Investigator looked into it. They felt that the payment of £21,000 to cryptocurrency was unusual and that Revolut should have spoken to Mrs B to carry out further checks on it. And they felt if this had happened, the scam would have been revealed. They also felt Mrs B should share liability for the loss so recommended a reduction in the reimbursement of 50%.

Mrs B accepted the findings, but Revolut did not. In summary, they felt the loss did not occur from the Revolut account so they should not be responsible for it, and that Mrs B was grossly negligent when she ignored warnings and selected an incorrect payment reason, amongst other things.

As an informal agreement could not be reached, the complaint has been 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 expressly requiring Revolut to refuse or delay a payment "*if legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks*".

So Revolut was required by the implied terms of its contract with Mrs B and the Payment Services Regulations to carry out their instructions promptly, except in the circumstances set out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

Whether or not Revolut was required to refuse or delay a payment for one of the reasons set out in its contract, the basic implied requirement to carry out an instruction promptly did not in any event mean Revolut was required to carry out the payments immediately¹. Revolut

¹ The Payment Services Regulation 2017 Reg. 86 states that "the payer's payment service provider must ensure that the amount of the payment transaction is credited to the payee's payment service

could comply with the requirement to carry out payments promptly while still giving fraud warnings, or making further enquiries, prior to making the payment.

And, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Revolut should in April 2023 fairly and reasonably have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances (irrespective of whether it was also required by the express terms of its contract to do so).

In reaching the view that Revolut should have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances, I am mindful that in practice all banks and EMI's like Revolut do in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;²
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system for authorised push payments;
- providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified.

In reaching my conclusions about what Revolut ought fairly and reasonably to have done, I am also mindful that:

- Electronic Money Institutions like Revolut are required to conduct their business with “due skill, care and diligence” (FCA Principle for Businesses 2), “integrity” (FCA Principle for Businesses 1) and a firm “must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems” (FCA Principle for Businesses 3)
- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the *“Financial crime: a guide for firms”*.
- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.

provider's account **by the end of the business day following the time of receipt of the payment order**” (emphasis added).

² For example, Revolut's website explains it launched an automated anti-fraud system in August 2018:

<https://www.revolut.com/news/revolut-unveils-new-fleet-of-machine-learning-technology-that-has-seen-a-fourfold-reduction-in-card-fraud-and-had-offers-from-banks/>

- The October 2017, BSI Code³, which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).
- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

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

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

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

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

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

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 is 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 in April 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, 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.

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 can see that Mrs B had an existing Revolut account that she used to facilitate the payments. Having compared the fraudulent payments to Mrs B's genuine account activity, I do not think the initial three payments were unusual enough to warrant intervention from Revolut prior to them being processed. This is because they were relatively low in value and were in line with the previous account activity.

However, I think the transfer of £21,000 was unusual due to the significant increase in value when compared to the genuine account activity. This was around 20 times higher than the regular payments Mr B made on the account and I think this jump was significant enough that Revolut should have taken steps to identify what the payment was for. This was also going to a known cryptocurrency exchange, which was out of character for Mrs B as the only payments to cryptocurrency on the account were in relation to the scam that she fell victim to.

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 am 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 and what kind of warning should they have provided?

For the transfer of £21,000 to the cryptocurrency wallet, Revolut provided Mrs B with a new payee warning that said:

“Do you know and trust this payee?

If you're unsure, don't pay them, as we may not be able to help you get your money back. Remember that fraudsters can impersonate others, and we will never ask you to make a payment”

While this warning does contain some information relevant to Mrs B's circumstances, the warning isn't particularly prominently displayed, requires no interaction or real engagement from the customer and, in my view, lacks sufficient context to have been impactful in the circumstances of this case.

Revolut also asked Mrs B to select the payment purpose for the £21,000 payment from a drop-down list, and she selected 'transfer to a safe account'. As a result, Mrs B was shown a warning relevant to safe account scams, which was not relevant to the scam she was victim to. Revolut have argued that Mrs B was negligent when she selected this option, as it did not match the purpose of the payment. While I recognise Mrs B could have selected that she was investing in cryptocurrency, I think that considering the high value of the payment in question, alongside the fact it was identifiably going to cryptocurrency, human intervention would have been a proportional intervention to the risk level the payment posed. I therefore think Revolut should have referred Mrs B to the in-app chat in order to get a better understanding of the purpose of the payment, to ensure she was not at risk of financial harm.

If Revolut had referred Mrs B to the in-app chat, would that have prevented the losses she suffered from the payment of £21,000?

When considering whether or not human intervention would have revealed the scam, I have considered the interactions between Mrs B and the scammer, as well as her interactions with the third-party bank I'll call 'L' that she used to fund the Revolut account.

After the first three payments, Mrs B no longer had any funds to put into the investment, The scammer therefore convinced her to take out a loan and she did so. She initially took out a £30,000 loan with L, followed by a further £5,000 loan a short while later. When Mrs B attempted to transfer the bulk of this loan over to Revolut, Mrs B was contacted by L on 9 May 2023 as they had fraud concerns. The scammer advised Mrs B to tell them the loan was for a car purchase and said the bank would try and convince her to invest with them instead if they knew about the investment.

I've listened to the phone call in question and Mrs B did set out that the transfer was for a car purchase. As a result, Mrs B was given a general safe account scam warning, but did not receive any warnings relevant to the scam she had fallen victim to. There was another call on 12 May that followed a similar pattern, with Mrs B explaining more funds were needed because the vehicle was more expensive than originally planned. Again, the call handler from L did not have any concerns and released the payment.

I've therefore considered whether an in-app intervention from Revolut when Mrs B made the

payment of £21,000 would have meaningfully revealed the scam. In doing so. I've considered the fact Mrs B followed the scammers instruction when speaking with L and misled them about the true purpose of the loan and the transfer to Revolut.

Looking at the chat with the scammer, I cannot see that Mrs B was given a cover story when making the payments to the cryptocurrency wallet. And as it was clear the payments were going to cryptocurrency, Mrs B would not have been able to use the same cover story that she was purchasing a car. While I do acknowledge that it is possible Mrs B could have been asked to lie to Revolut by the scammer had she been directed to the in-app chat, as the payment was not referred for further checks, this did not happen. So, based on what I've seen, I think it would have been clear that Mrs B was making a payment to a cryptocurrency exchange and nothing from the chat with the scammer indicates Mrs B was instructed to mislead Revolut in the circumstances.

Revolut have highlighted that when Mrs B made the payment of £21,000, she selected the payment purpose as 'safe account' and ignored the warnings she was provided. However, regardless of what Mrs B said the payment was for, I think it was clear the payment was going to cryptocurrency. Because of this, due to the risk payments to cryptocurrency exchanges posed along with the value of the payment, I think Revolut should reasonably have provided a clear warning that described the features of cryptocurrency investment scams. And the reason this did not happen when Mrs B spoke with L is because they did not have sight of the end destination of the funds.

On balance, I think there were a number of features of this scam that would likely be included in a cryptocurrency investment scam warning. For example, Mrs B was contacted out of the blue about an opportunity that boasted significant and unrealistic returns in a short amount of time. Also, she had been told to download screen sharing software, was instructed to borrow money to fund the investment and had been instructed to mislead her bank. On balance, I think a clear cryptocurrency scam warning would reasonably have mentioned enough of these features for the spell to be broken for Mrs B. I therefore think that had Revolut meaningfully intervened in the payment of £21,000 it is more likely the scam would have been revealed and further payments to the scam could have been prevented.

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

In reaching my decision about what is fair and reasonable, I have 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 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 taken into account that the final payment was made to another financial business (a cryptocurrency exchange) and that the payments that funded the scam were made from another account at regulated financial businesses.

But as I've set out 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 £21,000 payment, and in those circumstances Revolut should have made further enquiries about the payment before

processing it. If it had done that, I am satisfied it would have prevented the losses 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 Mrs B'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 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 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: 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 B's loss from the £21,000 payment (subject to a deduction for her 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 can see that Mrs B was invited to webinars about the investment, which I think would have given it an air of legitimacy. And from what I can see, it appears a genuine financial business was cloned to an extent to make the investment itself appear genuine.

However, the other features of the scam were indicative of a cryptocurrency investment scam and should reasonably have given Mrs B cause for concern. She was contacted out of the blue on a messaging app about the opportunity, which I think she could reasonably have seen as unusual. Following her initial investment, she quickly saw returns on the platform of over 10% over a short period of time, which I think she could have seen as too good to be true. By the time she made the payment of £21,000 Mrs B had been told she could repay a loan of £30,000 in just three months with the profits she could make, which means she was promised, in my view, significant and unrealistic returns.

Finally, Mrs B took steps to mislead her bank when taking out a loan to fund the investment. On balance, I think Mrs B should reasonably have thought something was not right when she was doing this. Having considered everything available to me I think it would be reasonable for Revolut to reduce the redress by 50%.

Putting things right

I uphold this complaint in part and require Revolut to:

- Refund Mrs B from the payment of £21,000 onwards, this redress can be reduced by 50% to account for Mrs B's shared liability for the loss.

- Pay Mrs B 8% simple interest on that refund, from the date of transactions until the date of settlement.

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

My final decision

For the reasons set out above, I uphold Mrs B's complaint in part. Revolut Ltd should now pay the redress outlined above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs B to accept or reject my decision before 20 February 2025.

Rebecca Norris
Ombudsman