

The complaint

Miss B is unhappy Revolut Ltd (“Revolut”) won’t reimburse her for the money she lost when she fell victim to a scam.

What happened

The details and facts of this case are well-known to both parties, so I don’t need to repeat them at length here.

In short, Miss B says she saw an advert for a trading company on social media that I will call “B”. Miss B completed an enquiry form and was contact by a representative of B.

Subsequently, the following transfers were made to a cryptocurrency exchange. My understanding is that the funds were then converted to cryptocurrency and were transferred on to B.

The following transactions went from Revolut to the cryptocurrency exchange.

Transaction Number	Date	Amount	Type of payment
1	8 May 2023	£756.14	Transfer
2	13 May 2023	£3,550	Transfer
3	15 May 2023	£4,500	Transfer
4	18 May 2023	£3,800	Transfer
5	18 May 2023	11,487.55 RON	Transfer
6	19 May 2023	£1,550	Transfer
7	23 May 2023	£2,550	Transfer
8	26 May 2023	£2,199	Transfer

Miss B realised that she had been scammed when she was repeatedly asked to send further funds but after sending the funds she remained unable to withdraw her “profits”. She was given a variety of reasons as to why the further payments needed to be made such as she needed to upgrade her trading account, that an IRS tax payment needed to be made, an anti-money laundering payment and a cost of transfer fee.

She made a complaint via a representative to Revolut and requested that the above transactions be refunded. It declined to do this.

One of our investigators looked into this matter and he thought that Revolut should have intervened during transaction 2 and had it done so, it would have prevented the loss that she suffered and that it should therefore refund all of the above payments. He did though say that there should be a deduction of 50% as he believed that Miss B was equally liable for her loss. Revolut did not agree and it said the following in summary;

- It has no legal duty to prevent fraud and it must comply strictly and promptly with valid payment instructions. It does not need to concern itself with the wisdom of those instructions. This was confirmed in the recent Supreme Court judgement in the case of *Philipp v Barclays Bank UK plc* [2023] UKSC 25.
- There are no legal obligations, regulatory obligations, industry guidance, standards or codes of practice that apply to Revolut that oblige it to refund victims of authorised push payment (“APP”) fraud. By suggesting that it does need to reimburse customers, it says our service is erring in law.
- Our service appears to be treating Revolut as if it were a signatory to the CRM Code. The Payment Service Regulator’s (“PSR”) mandatory reimbursement scheme will not require it to refund payments where the victim has ignored warnings with gross negligence. Miss B was grossly negligent by ignoring the warnings it gave and failing to carry out sufficient due diligence.

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 Miss 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 Miss 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 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 May 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.

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 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/>

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)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 Code⁴, 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 May 2023 that Revolut should:

³ 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.

⁴ 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.

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

It isn't in dispute that Miss 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 Miss 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 it upon which to discern whether any of the payments presented an increased risk that Miss B might be the victim of a scam.

Firstly, I don't think that Revolut would have had any reason to intervene in the first small payment that was made to the crypto exchange - mainly due to its size. That said I do think that it needed to intervene during payment 2. 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 the payments would be credited to a cryptocurrency wallet held in Miss B's name.

By May 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 transactions⁵. And by May 2023, when these payments took place, further restrictions were in place⁶. 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 prior to the payments Miss B made in May 2023, Revolut ought fairly and reasonably to have recognised that its customer could be at an increased risk of fraud when using its services to purchase cryptocurrency, and I think that's the case even though 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 (including the Consumer Duty), Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. And as I have explained Revolut was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks.

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

Payment 2 was clearly to a cryptocurrency exchange and was large enough in my view to have prompted an intervention from Revolut. The account was not new but had been rarely used. So two payments to a crypto exchange on a rarely used account within a few days of each other, for increasing amounts, should really have made Revolut aware that Miss B was at a heightened risk of financial harm.

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 Miss B?

⁵ 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.

⁶ In March 2023, Both Nationwide and HSBC introduced similar restrictions to those introduced by Santander in November 2022

I've gone onto consider whether the warnings that Revolut did give were proportionate to the risk the payment presented. I don't think they were. I'll explain why.

Revolut says it provided a warning to Miss B. The warning would have been displayed when she was creating a new payee, it read:

"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"

When the first payment was made Revolut's warning was in my view sufficient. But by payment 2 I don't think that this was sufficient.

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 Miss B attempted the second payment, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency 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; 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 Miss 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 Miss 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 Miss B's payments, such as finding the investment through social media, being assisted by a broker and being asked to download remote access software so they could help her open cryptocurrency wallet.

I've also reviewed the text conversation between Miss B and B. I've found nothing within those conversations that suggests Miss B was asked, or agreed to, disregard any warning provided by Revolut. I've also seen no indication that Miss 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 note Revolut's argument that Miss B continued sending funds to B after she first reported the scam to Revolut. I have carefully considered this and I don't think that Miss B actually was aware that she had been scammed when she first contacted Revolut via the in app chat. At this point she was concerned that she had to pay additional fees to B to release her "profits" she did not seem to think that the whole thing was a scam. I also note that Revolut did not at this point confirm that Miss B was being scammed. I note that she did mention during her conversations with B that she was concerned that she was being scammed but she is reassured by B. I also think that by the time Miss B first contacted Revolut, she was desperately trying to get her funds back and being told it was still possible to get her profits overrode her concerns. I think a warning from Revolut earlier in the scam, prior to Miss B sending so much to the scammer, would have carried more weight and likely stopped Miss B from sending further funds to the scammer.

In addition, Miss B did not receive any cryptocurrency investment related specific warnings from Revolut or the bank from which the money originated – so there's no evidence she ignored a specific warning.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Miss 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 based in another country) and that the payments that funded the scam were made from an account at a regulated financial businesses.

But as I've set out above, I think that Revolut still should have recognised that Miss B might have been at risk of financial harm from fraud when she made payment 2, 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 Miss 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 Miss B's own account, does not alter that fact and I think Revolut can fairly be held responsible for Miss 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 Miss 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 Miss B could instead, or in addition, have sought to complain against those firms. But Miss B has not chosen to do that and ultimately, I cannot compel them to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Miss 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 Miss B's loss from payment 2 (subject to a deduction for Miss B's own contribution which I will consider below).

Should Miss B bear any responsibility for their losses?

I've thought about whether Miss B should bear any responsibility for her loss connected to the scam. In doing so, I've considered what the law says about contributory negligence, as well as what I consider to be fair and reasonable in all of the circumstances of this complaint including taking into account Miss B's own actions and responsibility for the losses she has suffered.

In this instance Miss B doubled her money right at the start of the scam which is not something that a legitimate investment firm would likely be able to do. Also, it is unclear what, if any, research Miss B did whilst she was investing, as there is almost no information about the scammer online and as she had concerns during the scam being able to find nothing about B online should have been a red flag..

I am also mindful that Miss B had concerns as early as payment 2 about being scammed as she asked B whether she was being scammed at this point. I think her continuing to send payments despite her concerns means that she is equally liable for her loss from payment 2. I should highlight that I am not saying that Miss B knew she was being scammed and kept sending payments, I am saying that Miss B had concerns about B and failed to take steps to independently verify the legitimacy of the fraudster after having those concerns.

I've concluded, on balance, that Revolut can fairly reduce the amount it pays to Miss 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 Miss B's money?

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

The Faster Payments were sent to Miss B's own account at the cryptocurrency exchange, converted into cryptocurrency and then sent to the scammer. So I don't think that there was any way to recover the funds.

Putting things right

For the reasons I've explained, I uphold this complaint about Revolut Ltd in part and instruct it to do the following:

- 1) Refund 50% of the money Miss B lost to the scam from and including payment 2
- 2) Pay 8% simple interest per year on each payments from the date of the payments to 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 Miss B how much it's taken off. It should also give Miss B a tax deduction certificate if she asks for one, so she can reclaim the tax from HM Revenue & Customs if appropriate.

My final decision

My decision is that I uphold this complaint against Revolut Ltd in part and instruct it to do the following.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss B to accept or reject my decision before 27 November 2024.

Charlie Newton
Ombudsman