

The complaint

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

Subsequently, the following payments 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	4 April 2023	£3,000	Card Payment
2	23 April 2023	£1,400	Card Payment
3	23 April 2023	£1,800	Card Payment
4	23 April 2023	£1,300	Card Payment
5	23 April 2023	£150	Card Payment

Mrs K 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”.

I issued a provisional decision on 1 November 2024 in which I said the following;

“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 K 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 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;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 April 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat).

I 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".*

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/

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.

- *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 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;*

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

- *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 consumer was at risk of financial harm from fraud?

It isn't in dispute that Mrs K 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 K 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 Mrs K might be the victim of a scam.

The investigator has argued that Revolut should have intervened during payment 1 due to Mrs K mentioning that she was trading in crypto and naming B in an online chat with Revolut prior to this transaction.

I don't think though that Mrs K in the message exchange in the online chat made it clear that she was currently being scammed and as it did not relate to a payment that was being made from Revolut I don't think that it needed to intervene or ask more questions.

I don't think that it would have been reasonable to have expected Revolut to have examined a prior chat when a subsequent transaction was made unless the transaction merited a human intervention.

That said I still think that Revolut needed to intervene during payment 1 but not a human intervention a written warning was merited. I'm aware that cryptocurrency exchanges like B 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 Mrs K'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 transactions⁴. And by April 2023, when these payments took place, further restrictions were in place⁵. 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 K 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 (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 Mrs K might be at a heightened risk of fraud that merited its intervention.

⁴ 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.

⁵ In March 2023, Both Nationwide and HSBC introduced similar restrictions to those introduced by Santander in November 2022

I note that this was a new account and Revolut did not have a payment history to compare the payments to. But payment 1 was clearly to a cryptocurrency exchange and was large enough in my view to have prompted an intervention from Revolut. Given this I think that Revolut should have really been aware that Mrs K 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 which ought to have prompted a warning.

What did Revolut do to warn Mrs K?

My understanding is that Revolut did not provide with Mrs K with a warning for payment 1 or indeed the other payments

What kind of warning should Revolut have provided?

I've thought carefully about what a proportionate warning in light of the risk presented would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to this one will be entirely genuine. I've given due consideration to Revolut's duty to make payments promptly, as well as what I consider to have been good industry practice at the time this payment was made.

Taking that into account, I think Revolut ought, when Mrs K 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 Mrs K by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

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 K'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 e-mails between Mrs K and B. I've found nothing within those conversations that suggests Mrs K was asked, or agreed to, disregard any warning provided by Revolut. I've also seen no indication that Mrs K 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 also note that Mrs K did contact Revolut when she was having difficulty withdrawing her initial profits from the scam which shows that she trusted Revolut and was willing to be honest about what she was doing.

In addition, Mrs K 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 Mrs K's loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Mrs K 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 Mrs K might have been at risk of financial harm from fraud when they made payment 1, 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 K 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 K own account does not alter that fact and I think Revolut can fairly be held responsible for Mrs K'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 K 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 K could instead, or in addition, have sought to complain against those firms. But Mrs K 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 Mrs K'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 K's loss from payment 1 (subject to a deduction for Mrs K's own contribution which I will consider below).

Should Mrs K bear any responsibility for their losses?

I've thought about whether Mrs K 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 Mrs K's own actions and responsibility for the losses she has suffered.

Firstly I accept that this was a sophisticated scam and from what Mrs K has said B's website looked professional and convincing. But I think that there should have been a few red flags that should have concerned Mrs K.

In this instance Mrs K had already had trouble withdrawing her profits of around £1,000 before she made the first transaction from Revolut. This profit was made from an initial "investment" of around £160. This return is unrealistic given it was made in only a few weeks. And this should really have put her on notice that something may not be right which ought to have prompted her to make further enquires such as searching online. B has an FCA warning that is the first search result if you use an online search engine, so I don't think that Mrs K did sufficient research into B and she ignored the red flags of having difficulty withdrawing funds and having made unrealistic profits.

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

I've also thought about whether Revolut could have done more to recover the funds after Mrs K reported the scam. In this case Revolut raised a chargeback which was unsuccessful. I don't think that it needed to do more."

Neither party responded to my provisional decision by the deadline provided.

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.

Having reviewed everything, as neither party has provided any new information, I see no reason to reach a different outcome to the one I reached in my provisional decision.

So, in summary I think that Revolut should have intervened during payment 1 and this would have stopped the scam. I also think that Mrs K is partially responsible for her own loss.

Finally, I did not think that Revolut could have recovered the funds via other means.

Putting things right

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

- 1) Refund 50% of the money Mrs K lost to the scam from and including payment 1
- 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 Mrs K how much it's taken off. It should also give Mrs K 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 what I have set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs K to accept or reject my decision before 19 December 2024.

Charlie Newton
Ombudsman