

The complaint

Mrs D complains that Revolut Ltd won't refund money she lost when she fell victim to an investment scam.

Mrs D is being represented by solicitors in this complaint.

What happened

The detailed background to this complaint is well known to the parties and has been previously set out by the investigator. I'll only provide an overview and focus on giving my reasons for my decision.

The complaint concerns several electronic payments which Mrs D made from a newly created Revolut e-money account between May and June 2023. These were made in connection with an investment opportunity which Mrs D came across on a popular social media platform. After leaving her details, she was contacted by a representative of the company – I'll refer to it as "M" – who said they were her account manager.

Under the instructions of her manager, Mrs D set up an e-money account with Revolut and transferred funds from her account with her existing bank "N" to the new account. The money was then used to purchase cryptocurrency from a well-known cryptocurrency provider, before being sent to cryptocurrency wallets as instructed. The use of remote access software was involved.

Encouraged by profits made, Mrs D made further payments. Subsequently, when she requested a withdrawal, she was told she needed to pay various fees. Mrs D's husband suspected that she might have been scammed and told her not to make further payments. But Mrs D proceeded with paying the requested fees. When she was still unable to withdraw her profits and repeated chasers to her account manager were unsuccessful, Mrs D realised that she had been scammed.

The following payments are being disputed –

	Date	Amount
Payment 1	1 May	£2,000
Payment 2	3 May	£3,000
Payment 3	9 May	£2,000
Payment 4	11 May	£3,487
Payment 5	12 May	£4,013
Payment 6	12 May	£500
Payment 7	15 May	£1,000
Payment 8	22 May	£5,000
Payment 9	22 May	£5,000
Payment 10	6 June	£9,800
Payment 11	8 June	£4,900
Payment 12	8 June	£900

Payment 13	14 June	£3,500
Payment 14	19 June	£1,000
Payment 15	23 June	£4,000
	Total payments	£50,100

Revolut declined to refund any of the disputed payments, saying that Mrs D had authorised them. It said it asked Mrs D to confirm the payment purpose on two occasions (Payments 1 and 14) and provided a scam warning at these times. But she chose to proceed with the payments.

Our investigator concluded that Revolut ought to have taken additional steps when Mrs D attempted Payment 9 and this should have taken the form of a direct intervention instead of an automated warning. Had it done so, the investigator was persuaded that Mrs D would have stopped in her tracks and losses prevented. So, they asked Revolut to refund her losses (along with interest) from Payment 9 onwards.

Mrs D accepted the investigator's findings. But Revolut asked for the complaint to be decided by an ombudsman. In summary, it said the payments were self-to-self and the scam therefore didn't occur on Revolut's platform. Revolut said it is irrational and illogical to hold it liable for Mrs D's losses where it is merely an intermediate link.

I issued a provisional decision last month and gave reasons for why, although I intended upholding the complaint, the redress I planned on awarding was different to that recommended by the investigator.

I gave both parties an opportunity to provide any further comments or evidence for my consideration before I finalise my decision.

Mrs D's representative replied and said that she accepted my provisional decision.

We haven't heard back from Revolut despite sending a chaser prior to the deadline I gave. I've therefore assumed it has no further comments to make.

As I see no reason to depart from my initial findings, what follows is my provisional decision made final.

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 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 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 D 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 implied terms of its contract with Mrs D and the Payment Services Regulations to carry out her 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 didn't 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'm 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 at the time of these payments 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'm mindful that in practice all banks and EMIs 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;

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/

- 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'm 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.

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”

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-June 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 D was at risk of financial harm from fraud?

It isn't in dispute that Mrs D fell victim to a cruel scam. Nor is it disputed that she authorised the payments which she now seeks reimbursement for.

As the very first payment flagged as unusual on Revolut's fraud detection systems, and it recognised the transaction as possibly scam related, I've considered whether it intervened appropriately when it held the transaction and made further enquiries.

What did Revolut do to warn Mrs D?

After notifying Mrs D that the transaction could be a scam, Revolut asked her to select the payment purpose from a list of options. According to its system records, Mrs D selected *cryptocurrency*. Revolut says it showed Mrs D a series of 'educational screens' regarding the type of potential scam it identified based on her selection. But she chose to proceed with the payment regardless.

Revolut has provided a copy of the educational screens it says Mrs D would have seen at the time based on her selection:

Screen 1

*"Moving funds to your own account?
Please ensure no one besides you has access to that account"*

Screen 2

*"Asked to download a software?
If someone has asked you to download any software (like AnyDesk), this could be a scam!"*

Screen 3

*“Are you making a new investment?
Research if what you’re investing in is a legit company or cryptocurrency”*

Having thought carefully about this, I’m not persuaded that the content of Revolut’s educational screens was a proportionate response to the risk the transaction presented. Other than advising Mrs D to research the company she was investing in and telling her she *could* be scammed if she had been asked to download a remote access software (my emphasis), no specific context was given about how fraudsters attempted to defraud victims of cryptocurrency scams.

What kind of warning should Revolut have provided?

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.

By the end of 2022, 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. 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’m satisfied that by the end of 2022, prior to the payments Mrs D made, 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.

Given what I’ve said above about the prevalence of cryptocurrency scams, at the time of Mrs D’s payment, I consider a proportionate warning ought to have addressed the key risks and features of the most common cryptocurrency scams – cryptocurrency investment scams. The warning 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; returns that are too good to be true; the use of remote access software; and a small initial deposit which quickly increases in value.

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.

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 D by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

If Revolut had provided a warning of the type described, would that have prevented the losses Mrs D suffered?

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 D's payments, such as an advertisement promoted on social media, being assisted by a broker, and being asked to download remote access software so they could help her.

I've also reviewed the written conversation between Mrs D and the scammer (though I note that Mrs D appears to have also spoken to them, not just communicated through instant messages, and I haven't heard those conversations). I've found nothing within those conversations that suggests she was asked, or agreed to, disregard any warning provided by Revolut. I've also seen no indication that Mrs D expressed mistrust of Revolut or financial firms in general.

On the balance of probabilities, had Revolut provided Mrs D with an impactful warning that gave details about cryptocurrency investment scams and how she could protect herself from the risk of fraud, I believe it would have resonated with her. In making that finding, I'm mindful that Mrs D had just started investing. She's more likely to have heeded Revolut's warning at the initial stages of the scam when she hadn't parted with significant sums of money. Overall, I'm satisfied that a timely warning to Mrs D from Revolut would very likely have caused her to decide not to go ahead with Payment 1 – and subsequent payments – thereby preventing her loss.

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

In reaching my decision about what is fair and reasonable, I've taken into account that Mrs D 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've carefully considered Revolut's view that it was merely an intermediary and shouldn't be held responsible for the losses that occurred on a third-party site. But as I've set out in some detail above, I think that Revolut still should have recognised that Mrs D might have been at risk of financial harm from fraud when she the first payment flagged as suspicious, and it was notified that the transaction was cryptocurrency related. And in those circumstances, it should have taken additional steps before processing it. If it had taken those steps, I'm satisfied that it would have prevented the losses that Mrs D suffered. The fact that the money wasn't lost at the point it was transferred to the cryptocurrency provider doesn't alter that fact and I think Revolut can fairly be held responsible for Mrs D'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 the firm that is the point of loss.

I've also considered that Mrs D has only complained about 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 D could instead, or in addition, have sought to

complain against those firms. But Mrs D has not chosen to do that and ultimately, I can't 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 D'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've set out above, I'm satisfied that it would be fair to hold Revolut responsible for Mrs D's loss.

Should Mrs D 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.

It is clear that at the time of making these payments Mrs D believed M to be genuine. She's told us she researched the company online before deciding to invest. I've done a backdated search on the internet from around that time, and there is a lack of compelling adverse information about M that I could reasonably expect Mrs D to have found within the public domain at the material time. What I have seen instead are some positive Trustpilot reviews.

The persuasive and sophisticated techniques employed, including the provision of professional looking website and a trading platform which had all the features expected of an investment platform, led Mrs D to trust M and the information they were feeding her. I'm therefore satisfied there was no contributory negligence at the initial stage, as Mrs D was simply the unwitting and blameless victim of clever fraudsters. Revolut was the professional in financial matters; Mrs D was an unsuspecting layperson.

However, I do think that Mrs D should share responsibility for the losses suffered from Payments 13-15. These payments were sent in connection with paying the withdrawal fees. Reaching the chat correspondence between Mrs D and the scammer, on or around 12 June, she tells them that her husband has told her not to pay the fees as he suspects this is a con. Mrs D tells the scammer that her husband is contacting a friend who is a 'cyber specialist police'.

When questioned about this, her representative states that Mrs D didn't update her husband about her ongoing issues with the scammer and continued with the payments. I'm concerned that Mrs D's husband had misgivings which he shared with her, yet she went ahead with the last three payments. I consider it would have been reasonable to have carried out some independent due diligence. Had she done so, Mrs D would have seen the negative reviews that had appeared on Trustpilot and given her even more cause for concern.

Weighing up the liability that I've found on both sides with regards to Payments 13-15, I think a fair deduction is 50%.

Putting things right

To put things right for Mrs D, Revolut Ltd needs to refund all the disputed payments. It can however make a 50% deduction for Payments 13-15.

Revolut also needs to add simple interest at 8% per year to the individual refunded amounts, calculated from the date of loss to the date of settlement⁶.

My final decision

For the reasons given, my final decision is that I uphold this complaint. Revolut Ltd needs to put things right for Mrs D as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs D to accept or reject my decision before 9 April 2025.

Gagandeep Singh
Ombudsman

⁶ If Revolut considers that it's required by HM Revenue & Customs to deduct income tax from that interest, it should tell Mrs D 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.