DRN-5363484

The complaint

Miss S complains Revolut Ltd won't reimburse money she lost when she fell victim to a scam.

What happened

In April 2023 Miss S came across a success story on social media involving crypto trading with an organisation I will refer to as C. She researched into the company and reviewed the website. Miss S says she researched online reviews and could not find anything negative. So she completed an enquiry form and was subsequently contacted by C.

Miss S was happy with the information she received and agreed to sign up. She had access to a fake trading platform so she could see live trades which added to the belief that this was a genuine investment opportunity. As part of the scam, the scammer convinced Miss S to take loans out. Miss S made the following two payment as part of the scam:

Date	Type	Amount
15 April 2023	card	£10,000
21 April 2023	card	£5,000

Both payments were made to a genuine cryptocurrency provider (H) and from there the funds moved to a wallet under the control of the scammer.

Miss S could see her balance increase when deposits were made, and she could see profits and losses to the trades which added reassurance it was genuine. At the end of April 2023 Miss S requested a withdrawal but when she did not receive the money, she realised she was the victim of a scam and raised the matter with Revolut.

Revolut did not refund Miss S. It said the card payments in question were fully authorised by Miss S. It said it was used as an intermediary to receive funds from Miss S's main bank account which she then transferred on to a legitimate external account held with H. Miss S's money was lost further in the chain. It said Miss S did not question the unrealistic returns and there has been a lack of appropriate due diligence. Revolut doesn't believe it missed a chance to prevent any of the events related to Miss S's complaint.

Miss S bought her complaint to this service via a third-party representative. Our investigator did not uphold the complaint. Whilst he felt Revolut ought to have recognised the transaction was going to cryptocurrency, he didn't think any further intervention would have made a difference.

Miss S's representative asked for the matter to be referred for a decision. It felt Revolut could see the money was going to cryptocurrency and human intervention would have made the difference and Miss S would not have proceeded with the transactions. Just because Miss S was being coached by the scammer that should not free Revolut from any liability.

I issued my provisional decision on 13 February 2025 explaining why I was thinking reaching a different outcome to the investigator.

Miss S accepted my decision. Revolut did not respond.

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.

Revolut did not respond to my provisional decision.

Under the Dispute Resolution Rules (found in the Financial Conduct Authority's Handbook), DISP 3.5.13, says, if a respondent (in this case Revolut) fails to comply with a time limit, the ombudsman may proceed with the consideration of the complaint.

As the deadline for responses to my provisional decision has expired, I'm going to proceed with issuing my final decision. However, I think it's unlikely that Revolut would've provided any new evidence or information that would've changed the outcome of the case.

As neither party has provided any further evidence or arguments for consideration, I see no reason to depart from the conclusions set out in my provisional decision. For completeness, I have set this out below.

When considering what is fair and reasonable, I'm also required to take into account: relevant law and regulations; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the relevant 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 S 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:

[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_/

- Electronic Money Institutions like Revolut are required to conduct their business with "due skill, care and diligence" (FCA Principle for Businesses 2), "integrity" (FCA Principle for Businesses 1) and a firm "must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems" (FCA Principle for Businesses 3)[2].

- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the *"Financial crime: a guide for firms".*

- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.

- The October 2017, BSI Code[3], 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

[2] Since 31 July 2023 under the FCA's new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.
[3] BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

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.

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.

Whilst I am required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I am satisfied that to comply with the regulatory requirements that were in place in April 2023, Revolut should in any event have taken these steps.

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

It isn't in dispute that Miss S 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 we now know the circumstances which led Miss S 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 the payments presented an increased risk that Miss S might be the victim of a scam.

I'm understand that cryptocurrency platforms like H 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 S'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 transactions.

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 Miss S 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.

To be clear, I'm not suggesting as Revolut has argued that, as a general principle, Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees.

As I've set out in some detail above, it is the specific risk associated with cryptocurrency in April 2023 that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm.

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. 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.

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 the payments in this case were going to an account held in Miss S's own name should have led Revolut to believe there wasn't a risk of fraud.

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 S might be at a heightened risk of fraud that merited its intervention.

What did Revolut do to warn Miss S and were the steps it took sufficient?

Revolut says it provided a warning to Miss S when she set up H as a new beneficiary prior to making the payments. It says it warned Miss S that she might be falling victim to a scam by providing the following message:

"*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, fraudsters can impersonate others, and we will never ask you to make a payment"

It is very general in nature and it's difficult to see how it would resonate with Miss S or the specific circumstances of the transactions in question. Overall, I can't agree this was a proportionate response to the risk that the first payment presented. While I accept that Revolut has attempted some steps to prevent harm from fraud, the warning it provided was too generic to have the necessary impact, I think Revolut needed to do more.

I've thought carefully about what a proportionate intervention ought to have looked like, in light of the risk the payments presented. 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 primary duty to make payments promptly.

The payments were clearly going to a cryptocurrency provider. And whilst this was a new account with no account history, the account opening purpose was disclosed as "spending abroad". Neither the first payment for £10,000 (nor the brief activity beforehand) was in line with the stated account purpose. Given the amount and what Revolut knew (or strongly suspected) that the payment was going to a cryptocurrency provider, I'm satisfied that Revolut should have identified both payments carried a heightened risk of financial harm and in line with good industry practice and regulatory requirements, I am satisfied that it is fair and reasonable to conclude that Revolut should have intervened further before the first payment went ahead.

To be clear, I do not suggest that Revolut should intervene for every payment made to cryptocurrency. Instead, as I've explained, I think it was a combination of the characteristics of this payment - such as the amount (combined with those which came before it, such as the stated account opening purpose, and the fact the payment went to a cryptocurrency provider) which ought to have prompted a staff intervention – for example reaching out to Miss S through its in-app chat function.

For the reasons I've set out above I'm satisfied that by April 2023, Revolut should have recognised at a general level that its customers could be at increased risk of fraud when using its services to purchase cryptocurrency and, therefore, it should have taken appropriate measures to counter that risk to help protect its customers from financial harm from fraud.

Such proportionate measures would not ultimately prevent consumers from making payments for legitimate purposes.

If Revolut had intervened as set out above, would that have prevented the losses Miss S suffered from the first payment?

I've thought carefully about whether a staff intervention with questions and warnings around 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 S's payments, such as finding the investment through an advertisement on social media, being assisted by an 'adviser' and being asked to download remote access software so they could help her open cryptocurrency wallets.

I've also reviewed the limited text conversation between Miss S and the fraudsters (though I note that Miss S appears to have spoken to the fraudster, not just communicated by instant message, and I haven't heard those conversations).

I am also aware that Miss S gave her high street bank a cover story for the transactions which were the source of these funds when she tried to transfer them into her Revolut account. That story centred around helping a friend who had been stranded by her husband abroad. I do appreciate Miss S was prepared to mislead her high street bank (albeit this was likely under the instruction of the scammer) and so the same might apply to Revolut. So I can understand why the investigator felt Miss S might have continued to conceal the real reasons for the payment purpose. I have considered this point carefully.

I can see within the messages with the scammer the scammer told Miss S "*usually we use mediator banks to avoid trouble with the major ones as they are against cryptocurrency trading*." And so, I think it's quite plausible Miss S would have been more honest with Revolut given the concerns where primarily with not disclosing the real reasons for the transactions with her high street bank.

But perhaps more significantly, I think the cover story (or any alternative cover story) would have very quickly fallen apart here, as Revolut could see where the money was going and so the potential scam risk was clearly apparent from the destination of the payments.

Therefore, on the balance of probabilities, had Revolut probed Miss S more about the payments with open questions and provided impactful warnings about cryptocurrency investment scams and how she could protect herself from the risk of fraud, I believe it would have resonated with her. She could have paused and looked more closely into C before proceeding. Whilst the name of the advisor appears to have been associated with a genuine name on the FCA register, there was a warning about C itself. I'm satisfied that a timely warning to Miss S from Revolut would very likely have caused her to take the steps she did take later – revealing the scam and preventing her further losses.

Overall, I think that staff intervention and a warning provided by Revolut would have given the perspective Miss S needed, and she would more likely than not have concluded that the scheme was not genuine. In those circumstances I think, she's likely to have decided not to go ahead with the payments, had Revolut intervened in person (for example via its in-app chat function) and such a warning been given.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Miss S 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 payment were made to another financial business (a cryptocurrency platform) and that the payments that funded the scam were made from other accounts at regulated financial businesses in Miss S's name.

But as I've set out in some detail above, I think that Revolut still should have recognised that consumer might have been at risk of financial harm from fraud when she made the payments, and in those circumstances, it should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it would have prevented the losses consumer suffered. The fact that the money used to fund the scam came from elsewhere and/or wasn't lost at the point it was transferred to consumer's own account does not alter that fact and I think Revolut can fairly be held responsible for consumer'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 consumer 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 consumer could instead, or in addition, have sought to complain against those firms. Miss S's high street bank did intervene, but it wasn't aware of what Revolut was aware of – ie that the final destination of the payment was cryptocurrency. Ultimately the consumer has not chosen to complain, and 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 consumer'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 consumer's loss for both payments (subject to a deduction for consumer's own contribution which I will consider below).

Should Miss S bear any responsibility for her losses?

I've thought about whether Miss S should bear any responsibility for her loss connected to the payments. 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 S's own actions and responsibility for the losses she has suffered.

I recognise that there were relatively convincing aspects to this scam such as the name of the individual working for C appears to be associated with a genuine authorised individual. I can imagine this would have given some validation to the person she was dealing with. But the opportunity arose through social media and Miss S was encouraged to take out loans to make the investment. Miss S said herself when reporting the matter to Revolut that she didn't get the scammer to email her over the process before going ahead. She said she "was

very sceptical, sadly did not go with my gut instinct." Miss S said she did check out C and found nothing of concern but there was an FCA warning about C itself - which would have appeared under a quick internet search. The fact that Miss S was told by the scammer that her mainstream bank would be concerned about payments to cryptocurrency ought to have been something Miss S should have questioned further.

So, given the above, I think she ought reasonably to have realised that there was a possibility that the scheme wasn't genuine and made additional enquiries. In those circumstances, I think it fair that she should bear some responsibility for her losses.

I've concluded, on balance, that it would be fair to reduce the amount Revolut pays Miss S in relation to both payments 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 to recover Miss S's money?

The payments were made by card to a cryptocurrency provider. Miss S sent that cryptocurrency to the fraudsters. So, Revolut would not have been able to recover the funds. In addition, I don't consider that a chargeback would have had any prospect of success given there's no dispute that H provided cryptocurrency to Miss S, which she subsequently sent to the fraudsters.

Putting things right

Revolut Ltd should put things right for Miss S by

- Refunding 50% of both transactions – so £7,500

- Because Miss S has been deprived of this money, I consider it fairest that Revolut Ltd add 8% simple interest to the above from the date of the transactions to the date of settlement.

If Revolut is legally required to deduct tax from the interest it should send Miss S a tax deduction certificate so she can claim it back from HMRC if appropriate.

My final decision

My final decision is that I uphold this complaint in part, and I require Revolut Ltd to put things right for Miss S as set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss S to accept or reject my decision before 28 March 2025.

Kathryn Milne
Ombudsman