DRN-4937518

The complaint

Mrs R complains that Revolut Ltd won't refund money she lost when she fell victim to a cryptocurrency investment scam.

What happened

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

The complaint concerns six payments totalling £31,850 which were made from Mrs R's Revolut account in March 2023. They were sent in connection with an investment opportunity with a company "B" whose advertisement Mrs R came across on an online website. After signing up, Mrs R was contacted by a representative of the company who said they were her trading manager and would place trades on her behalf. Mrs R says she researched B online, and its website said it provided traders with cutting-edge trading platforms to trade and other financial instruments across global markets. She says she felt she could trust the company.

Mrs R says her manager asked her to let them have control and they would show her how it all worked. She also states that the representative was very convincing and rang her daily to add more trades and show her how her profits were rising. They convinced her to spend more money by telling her she wouldn't be able to draw her winnings if she didn't.

Then one day, another representative from B phoned Mrs R and informed her that her trading manager had done something untoward. Mrs R was told she needed to pay more money in to get all her money back – it was explained to her that this additional payment was to pay taxes. When she told B she didn't have any more money left, Mrs R was encouraged to apply for a loan. She states she refused to do this, and the representative lost their temper. It was at this point that Mrs R realised she'd been scammed.

The following transactions are being disputed –

	Date	Type	Merchant/Payee	Amount
Payment 1	6 March	Debit card	Crypto provider 1	£2,500
Payment 2	15 March	Debit card	Crypto provider 2	£2,250
Payment 3	16 March	Debit card	Crypto provider 2	£2,600
Payment 4	22 March	Transfer	Crypto provider 3	£12,000
Payment 5	23 March	Transfer	Crypto provider 3	£9,000
Payment 6	23 March	Transfer	Crypto provider 3	£3,500
			Total payments	**£31,850**

Revolut declined to refund any of the disputed payments, saying Mrs R had authorised them. It also said that it provided a new beneficiary warning when she attempted Payment 4 – after asking Mrs R to confirm the payment purpose, it provided a scam warning over a series of educational screens, but she chose to proceed.

Our investigator didn't think the first three transactions were that unusual such that Revolut ought to have been concerned. Payment 4 should and did flag as suspicious. But the investigator thought that an appropriate intervention from Revolut would have been a human intervention by a member of staff. And further questions should have been asked about the flagged payment. Had that happened, the investigator was persuaded that the scam would have unravelled, and further losses prevented. They asked Revolut to refund Mrs R's loss (along with interest) from that payment onwards.

Mrs R accepted the investigators findings. She also said she had no recollection of being involved with any of the disputed transactions and believed the scammer was able to remove money from her Revolut account with her permission.

Revolut disagreed with the investigator's conclusions. In summary, it said these were self-to-self transactions and the scam didn't occur on its platform.

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.

I'd like to start by thanking both parties for their continued patience while waiting for the complaint to be reviewed by an ombudsman.

I can see Mrs R is now disputing having any involvement with the payments in question. The relevant law here is the Payment Services Regulations 2017 – these set out what is needed for a payment to be considered authorised and who has liability for disputed payments in different situations. With some exceptions, the starting point is that the consumer is responsible for authorised payments and the business is responsible for unauthorised payments.

For a payment to be authorised, it must be consented to by the consumer or someone acting on their behalf. This consent must be given in the form and in accordance with the procedure agreed between the consumer and the business.

It isn't in dispute that Mrs R fell victim to a cruel scam. I can see that she's told us she was tricked into granting remote access to the scammer. But Revolut has said that due to limitations, it is impossible for a third party to have taken control of its app on Mrs R's mobile phone. What that means is the approvals for card payments and the transfers – which is how the transactions in question were authenticated – could not have been completed by the scammer through remote access software which Mrs R was tricked into downloading.

I've reviewed the evidence – screenshots – that Mrs R shared with Revolut at the time of reporting the scam. I think it's clear from her written correspondence with the scammer that Mrs R would have been aware that funds were leaving her account. For instance, on 20 March 2023, the scammer says, *"… maybe we can make a 2nd transfer for the same amount…."*. And, later that day, Mrs R asks how much money is in her wallet and the scammer says the amount that will be sent.

I acknowledge that its possible Mrs R didn't fully understand the mechanics of how the investment worked. But given what I've said about how the transactions were authenticated, the limitations on the use of remote access on the Revolut app, and the correspondence between her and the scammer, on balance, I think Mrs R did authoriser the transfers.

As for the card payments, I accept that the scammer most likely completely some of the steps involved. For instance, entering the card details on the cryptocurrency provider's website or app to give the payment instructions. But Mrs R needed to have approved the payments in her Revolut app for them to be processed. By doing this, she made a representation to Revolut that the payment instruction was made by someone acting on her behalf. So, I think it is reasonable that the card payments are also considered authorised.

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 R 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"* (section 20).

So Revolut was required by the implied terms of its contract with Mrs R 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 immediately[1]. 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

[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).

should in March 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'm mindful that in practice all banks and EMIs like Revolut did 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.

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 don't 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[4], 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

[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_/

[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"

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 March 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 R was at risk of financial harm from fraud and were the steps it took to warn her sufficient?

By March 2023, when these transactions occurred, 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[5]. And by March 2023, further restrictions were in place[6]. This left a

[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.

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 R 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.

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 Mrs R'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 Mrs R might be at a heightened risk of fraud that merited its intervention.

I don't think there was anything particularly unusual about the card transactions (Payments 1-3) such that I think they ought to have flagged as suspicious on Revolut's systems. By the time Mrs R authorised the first transfer (Payment 4), I think Revolut ought to have recognised that she was at heightened risk of financial harm from fraud. The transaction value – £12,000 – was significantly higher (more than double) than any spending activity on the account in the previous 12 months. Also, there were declined card transactions to cryptocurrency providers for the same amount just prior to the transaction in question.

Given what I've noted above, in line with good industry practice and regulatory requirements, I'm satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before Payment 4 payment went ahead. The transaction did flag as unusual on Revolut's fraud detection systems. As Revolut recognised the transaction as possibly scam related, I've considered whether it intervened appropriately when it held the transaction and made further enquiries.

As I've mentioned, just prior to Payment 4, several card payments to a cryptocurrency provider were declined by Revolut. Based on the information I've seen, Revolut froze Mrs R's card. In its final response letter to Mrs R's representative, Revolut said it showed a message about the payment purpose and displayed educational screens covering the potential scam identified. But it hasn't provided our service with any information or evidence regarding the steps it took when it declined the card payments.

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.

In relation to Payment 4, Revolut says that after notifying Mrs R that the transaction could be a scam it asked her to select the payment purpose from a list of options. It says it then displayed a warning relevant to the option chosen. According to a system screenshot Revolut has provided, 'cryptocurrency' was selected as the payment purpose at the time. But Revolut hasn't provided us a copy of the warning it says it would have shown Mrs R before giving her the option to cancel or continue with the payment.

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 good industry practice at the time this payment was made.

Revolut has told us it presented Mrs R with warnings both at the time of the attempted card payments and when Payment 4 was made. But it hasn't shared with us what those warnings would've said. Having thought carefully about what Revolut knew of these payments and so the risk the transactions presented (including their value and the destination), I don't consider an automated warning about the scam risk identified could be a proportionate response to that risk. I think Revolut needed to do more in the situation.

Although Revolut hasn't shared the content of the warnings it says it would have shown Mrs R – either at the time of the attempted card payments or Payment 4 – having thought carefully about the risk the transactions presented (including their value and the destination), I don't consider an automated warning about the scam risk identified could be a proportionate response to that risk. I think Revolut needed to do more in the situation.

I think a proportionate response to the risk would be for Revolut to have attempted to establish the circumstances surrounding the transaction before allowing it to debit Mrs R's account. I think it should have done this by, for example, directing Mrs R to its in-app chat to discuss the payment further. In making that finding that

If Revolut had attempted to establish the circumstances surrounding Payment 4, would the scam have come to light and Mrs R's losses been limited?

Had Revolut asked Mrs R to provide further details of the payment she'd just attempted, I've no reason to believe she wouldn't have confirmed she was purchasing cryptocurrency. After all, she selected that option when presented with the list of options prior to Revolut's automated warning.

I would have then expected the agent to have probed further, having noted the increased cryptocurrency spending in the preceding days (the disputed card payments) as well as the unsuccessful card payments earlier that day. Had it done so, on balance, I think Mrs R would have told Revolut why she was purchasing cryptocurrency. I think she would have also mentioned the involvement of a third-party broker who had been assisting her. I say this because I've found nothing in the written correspondence between Mrs R and the scammer that she was coached to hide the true purpose of the payments.

I note that Mrs R appears to have also spoken to the scammers, not just communicated through instant messages, and I haven't heard those conversations. But there's no suggestion that she agreed to disregard any warning provided by Revolut. I've also seen no indication that Mrs R expressed mistrust of Revolut or financial firms in general. On the contrary, from what I've seen, when she was encouraged to apply for a loan to continue making payments and put down an inaccurate reason for the loan purpose, Mrs R refused to do that.

There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Mrs R's payments, such as being assisted by a broker who offered to trade on her behalf and being asked to install remote access software. I think Revolut would have immediately recognised that she was falling victim to a scam and would have been able to provide a very clear warning.

Given that Mrs R had no desire to lose her money, on balance, I think its very likely she would have stopped and not followed the scammer's instructions. And her losses from that point would have been prevented. So, I'm satisfied that an intervention of the type described above would have been more impactful and led to Mrs R responding positively.

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

In reaching my decision about what is fair and reasonable, I've taken into account that Mrs R purchased cryptocurrency which credited an e-wallet held in her own name, rather than making a payment directly to the scammer. 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 the fraudulent activity didn't occur on its platform.

However, for the reasons I have set out above, I'm satisfied that it would be fair to hold Revolut responsible for Mrs R's losses from Payment 4 onwards. As I've explained, the potential for multi-stage scams, particularly those involving cryptocurrency, ought to have been well known to Revolut. And as a matter of good practice, I consider it fair and reasonable that Revolut should have been on the look-out for payments presenting an additional scam risk including those involving multi-stage scams.

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 R's own account doesn't alter that fact and I think Revolut can fairly be held responsible for her 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.

Our service did contact the other firm involved and there were no claims or interventions to note. I've also considered that Mrs R has only asked us to consider her complaint against Revolut. She hasn't chosen to complain to the other financial institutions and ultimately, I can't compel her to.

I'm not persuaded that it would be fair to reduce Mrs R's compensation in circumstances where: the consumer has only complained to our service about one respondent from which they are entitled to recover their losses in full; 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) and for the reasons I have set out above, I'm satisfied that it would be fair to hold Revolut responsible for Mrs R's loss from Payment 4.

Should Mrs R 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 I consider to be fair and reasonable in the circumstances of this complaint.

Having considered the matter carefully, I don't think that there should be any deduction from the amount reimbursed. There were aspects to the scam that would have appeared convincing. Mrs R came across the investment opportunity through an advertisement on an online website. I haven't seen this advertisement, but I've seen other examples. In my experience, they often appear as paid advertisements on social media websites and a reasonable person might expect such advertisements to be vetted in some way before being published. Those adverts also can be very convincing – often linking to what appears to be a trusted and familiar news source.

I've also taken into account the provision of the trading platform (which, I understand, used genuine, albeit manipulated, software to demonstrate the apparent success of trades). I know that the scammer used the apparent success of early trades to encourage increasingly large deposits.

Mrs R states she reviewed B's website before deciding to go ahead. I think she could have researched into customer reviews about the company. But having done a backdated internet search, I can't see any adverse information about B in the public domain prior to Mrs R's payments. So had she carried out further due diligence on B, I'm not satisfied that she would have come across anything that ought to have concerned her. A scam warning was published by the UK financial services regulator, but that wasn't until weeks after Mrs R's final payment. By that point, she'd already reported the matter to Revolut.

Revolut argues that there were payments to other investment platforms prior to the disputed payments. I've carefully considered its comments. I note that there were two payments to a different investment platform in February 2023, i.e., a month prior to the scam payments. One of these transactions was reversed. Mrs R has said she was looking into investing around the time the scam occurred. So, it's not surprising that payments to other investment platforms were made from her Revolut account.

But I don't think it's fair to say that two previous payments automatically means Mrs R was an experienced investor and should therefore have been more cautious about the circumstances in which the opportunity was presented. I think there's a big difference in making two payments (one of which ended up being reversed) and the account showing a history of regular investment-related payments.

Overall, I don't think there should be a deduction to the amount reimbursed. Mrs R clearly didn't want to lose her money. Her actions cannot be explained by carelessness or personal gain. There's little other explanation than that she believed what she was told by some very sophisticated scammer. In the circumstances I don't find her belief to be unreasonable.

Could Revolut have done anything else to recover Mrs R's money?

Mrs R made card payments to purchase cryptocurrency. I'm not persuaded there would have been any reasonable prospect for a chargeback claim succeeding, as the merchant would be able to demonstrate that it had provided the goods/services that had been purchased using the card (in this case, the cryptocurrency that was then sent on to the scammer).

As for the transfers, I can see Revolut did contact the beneficiary account provider. But the funds had already been moved out (to purchase cryptocurrency).

So, I don't think there was anything more Revolut could have done to recover the money in these circumstances.

Putting things right

Revolut Ltd needs to refund Mrs R Payments 4-6 (inclusive). It also needs to add simple interest at 8% per year to the refunded amount, calculated from the date of loss 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 R how much it's taken off. It should also give her a tax deduction certificate if she asks for one, so she can reclaim the tax from HM Revenue & Customs if appropriate.

My final decision

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

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

Gagandeep Singh
Ombudsman