DRN-5558397

The complaint

Mrs R complains that Revolut Limited won't reimburse her after she fell victim to an investment scam, followed by further recovery scams.

Mrs R is professionally represented in bringing her complaint, but for ease of reading, I'll refer to all submissions as being made by Mrs R directly.

What happened

On 29 April 2025, I issued my provisional decision on this complaint. I wanted to give both parties a chance to provide any more evidence and arguments before I issued my final decision. That provisional decision forms part of this final decision and is copied below.

The details of this complaint are well known to both parties and have been set out already in detail by the investigator so I don't intend to repeat them here. But briefly, both parties accept that Mrs R contacted, what she believed was an investment firm, after seeing them advertised on social media, with a supposed celebrity endorsement. However, unfortunately this 'firm' was in fact a scam. She deposited funds with the fraudster believing she was investing in cryptocurrency, but realised she'd been scammed after she lost all her funds.

Mrs R was then contacted by fraudsters purporting to work for a recovery firm, claiming they could recoup her money sent to the scam investment. After sending funds to this firm to recover her money, with nothing ever materialising, Mrs R realised she'd fallen victim to another scam. Mrs R then contacted a second scam recovery firm who she found online, who committed the same scam on her again.

Mrs R made the payments to the fraudster from her Revolut account, which she was instructed to open by the fraudster. Mrs R was advised to purchase cryptocurrency, and then directed on how to transfer the cryptocurrency from her own wallet to those controlled by the fraudster. Only one payment towards the end of the scam was made by bank transfer. Mrs R complains that Revolut ought to have questioned the volume of payments being made from her account towards cryptocurrency and had it done so, she considers the scam would've come to light.

In total, the following payments were made towards the scam:

Date	***Destination***	***Payment value***
20/03/2023	*Cryptocurrency wallet one*	*£2,500*
22/03/2023	*Cryptocurrency wallet one*	*£5,000*
22/03/2023	*Cryptocurrency wallet one*	*£9,000*
28/03/2023	*Cryptocurrency wallet one*	*£7,000*
06/04/2023	*Cryptocurrency wallet one*	*£3,000*
14/04/2023	*Cryptocurrency wallet one*	*£8,780*
06/05/2023	*Cryptocurrency wallet one*	*£6,428*
06/05/2023	*Cryptocurrency wallet one*	*£8,571.43*
10/05/2023	*Cryptocurrency wallet one*	*£600*
10/05/2023	*Cryptocurrency wallet one*	*£5,000*

27/05/2023	*Cryptocurrency wallet one*	*£5,500*
10/06/2023	*Cryptocurrency wallet one*	*£1,204.65*
10/06/2023	*Cryptocurrency wallet one*	*£8,000*
23/07/2023	*Cryptocurrency wallet two*	*£1,251.33*
25/07/2023	*Cryptocurrency wallet two*	*£1,256.48*
29/08/2023	*Cryptocurrency wallet two*	*£8,239.20*
11/09/2023	*Faster payment to new payee*	*£3,826.60*
24/09/2023	*Cryptocurrency wallet two*	*£128.20*
	Total	***£85,285.89***

Revolut considered Mrs R's complaint but didn't uphold it. It said all card payments were authorised by Mrs R and were made to legitimate merchants. When making the bank transfer, Revolut has confirmed it provided the following warning:

*'**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 therefore considers Mrs R was appropriately warned against making the transfer.

Additionally, in its file to our service, Revolut made the following points:

- *Revolut recognises its obligations to have adequate procedures in place to counter the risk that it may be used to further financial crime, but that duty is not absolute and does not go as far to require Revolut to detect and prevent all fraud. It must comply with valid payment instructions and does not need to concern itself with the wisdom of those instructions. This was confirmed in the recent Supreme Court judgement in the case of Philipp v Barclays Bank UK plc [2023] UKSC 25.*

- *Our service has overstated Revolut's duty to Mrs R, and erred in law, by stating that Revolut ought to have done more in this case.*

- *Mrs R's external bank would have a better overall view of her spending behaviour and transactions leaving that account would have been objectively more suspicious.*

- *These were self-to-self payments, and it is irrational for Revolut to be held liable for losses where it was merely an intermediate link.*

Mrs R remained unhappy and referred her complaint to our service. An investigator considered the complaint but didn't uphold it. She thought that Revolut ought to have intervened more than it did when Mrs R made the scam payments. However, the investigator noted that Mrs R had questioned whether she was being scammed several times and continued making payments. Mrs R also misled Revolut on questions it posed to her in September 2023 of the scam, when she advised she hadn't downloaded screen sharing software, but this doesn't appear to be the case. The investigator therefore considered that even if Revolut had intervened further, Mrs R would've proceeded, in spite of any warnings provided.

Mrs R disagreed with the investigator's view. She said that Revolut's questioning was too late into the scam, when Mrs R had already lost her money to the investment scam and was desperate to recover it. She considers that had Revolut intervened sooner and provided a cryptocurrency investment warning, this would've been sufficient to break the spell.

As Mrs R remains unhappy, the complaint has been referred to me for a final decision.

What I've provisionally 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 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 – 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 (and refused or delayed payment transfers) 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 March 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 do 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 March 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).*

- *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.*

[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_/

- *The October 2017, BSI Code[2], 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[3] 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 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*

---

[2] BSI: PAS 17271: 2017" Protecting customers from financial harm as result of fraud or financial abuse"

[3] Keeping abreast of changes in fraudulent practices and responding to these is recognised as key in the battle against financial crime: see, for example, paragraph 4.5 of the BSI Code and PRIN 2A.2.10(4)G.

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 March 2023, Revolut should in any event have taken these steps.

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

It isn't in dispute that Mrs R has fallen victim to a cruel scam here, nor that she authorised the payments she made by card to her cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer), as well as the later payment transfer.

Whilst I have set out in this decision the circumstances which led Mrs R 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 R might be the victim of a scam.

I'm aware that cryptocurrency exchanges generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. Revolut would likely have been aware of this fact too. So, it could have reasonably assumed that payments would be credited to a cryptocurrency wallet held in Mrs R's name.

By March 2023, when these transactions began, 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[4].

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.

[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.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mrs R made from March 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 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 by March 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. 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 think Revolut should have identified that all card payments were going to a cryptocurrency provider (the merchants are well-known cryptocurrency providers). I appreciate that Revolut has stated that this was a newly opened account and therefore there was no transactional history available about Mrs R. However, as I've already set out, based on the known risks surrounding cryptocurrency payments, as well as an identified increase in EMIs being used as an intermediate step between high street banks and cryptocurrency wallets, I think there was still a point where Revolut should have intervened and further questioned Mrs R.

Given what Revolut knew about the destination of the payments, I think that by the time Mrs R made the second payment towards the scam, the overall circumstances should have led Revolut to consider that Mrs R was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements, I am satisfied that it is fair and reasonable to conclude that Revolut should have warned Mrs R before this payment went ahead.

To be clear, I do not suggest that Revolut should provide a warning for every payment made to cryptocurrency. On the contrary, as I've explained above, I don't think the first payment Mrs R made towards the scam was unusual enough that it required intervention. Instead, as I've explained, I think it was a combination of the characteristics of this second payment (a newly set up account with payments being made in from another banking provider, then being sent straight on to cryptocurrency in high value payments) which ought to have prompted a warning.

<u>What did Revolut do to warn Mrs R and should it have done more in the circumstances?</u>

Revolut has confirmed that before allowing a payment to be made to a new payee (so for the payment transfer on 11 September 2023) it provided the following warning to Mrs R:

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

Additionally, I can see from the chat transcript between Mrs R and Revolut that a payment attempted on 29 August 2023 was declined by Revolut, which Revolut advised was 'due to its possible high risk nature' and that other payments to this beneficiary may also be blocked. However, it doesn't appear any further warning about the risks involved were communicated to Mrs R.

It also appears Mrs R tried to make a faster payment on 18 September 2023 but this was temporarily stopped by Revolut for further checks. Revolut explained that Mrs R had confirmed during questions that she had been asked to install remote access software and was concerned Mrs R was being scammed. It asked her to uninstall any software and to stop speaking to anyone immediately who had asked that she install it. Mrs R advised that she had pressed this option by mistake and no one had asked her to install software. Mrs R's payment was eventually released back to her account.

It doesn't appear Revolut questioned any of the card payments Mrs R made, so 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 these will be entirely genuine. I've given due consideration to Revolut's primary duty to make payments promptly.

Taking that into account, I think Revolut ought, when Mrs R attempted to make the second scam payment of £5,000 on 22 March 2023, knowing 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, often using celebrity endorsements, 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 R by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

<u>If Revolut had provided a cryptocurrency investment scam warning, would that have prevented the losses Mrs R incurred?</u>

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 R's payments, such as an online advertisement with endorsements, the use of an account manager, unrealistic returns and screen sharing applications.

I've thought about how Mrs R may have responded to such a warning being presented on payment two of the scam. I've thought about the fact that Mrs R had clear doubts about whether she was being scammed by the time she was sending funds to the 'recovery agents', but proceeded in spite of these concerns. However, I don't think her actions at this point of the scam are a fair reflection of how she may have acted in the early stages of the scam. I say this because by the time the first recovery scam began, Mrs R had already lost around £70,000, was in debt and, from reviewing the chats she had with the fraudsters, appears to be in a vulnerable financial position and desperate to recoup some of her funds. While I agree that by this time, it probably would've been quite difficult for Revolut to have 'broken the spell' of the fraudster, I don't think this same logic applies to earlier intervention when Mrs R was less entrenched, and with less to lose.

Unfortunately, as Revolut didn't provide warnings for any of the card payments Mrs R made, I'll never know with any certainty how Mrs R would've responded to such a warning. However, as the scam was typical in its setup for a cryptocurrency investment scam – which is what I think Revolut ought to have warned against – I see no reason to determine that Mrs R wouldn't have responded positively to such a warning. I've also not seen evidence that Mrs R was being coached by the fraudster on how to make the payments.

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 have 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 fraudsters. So the funds passed through an additional financial institution before losses were incurred.

I have carefully considered Revolut's view that in a multi-stage fraud, liability for any losses incurred should be recoverable against the financial institution where the loss occurred.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mrs R might have been at risk of financial harm from fraud when she made the second payment towards the scam, 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 further losses Mrs R suffered. The fact that the money wasn't lost at the point it was transferred to Mrs R's own cryptocurrency account does not alter that fact and I think Revolut can fairly be held responsible for Mrs R'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.

In this case, Mrs R has also complained about the account provider from which funds originated, and I have provisionally held it liable in part also for Mrs R's losses. I've covered what this means for Revolut's liability in more detail further below.

While I accept that it's possible that further firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, 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 R's loss from the second successful payment she made to the scam (subject to a deduction for her other banking provider's contributions, as well as Mrs R's own contribution which I will consider below).

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's fair and reasonable in the circumstances of this complaint.

Mrs R has explained she saw the initial investment opportunity advertised online, with a celebrity endorsement. While I can entirely appreciate the reassurance this would have provided to Mrs R, I also think Mrs R ought to have conducted her own research online, prior to proceeding with significant payments towards the scam. I also wouldn't consider the manner in which the fraudster spoke with Mrs R to be professional and what would be expected from an account manager and it doesn't appear she ever received any returns to demonstrate that the money she was making did in fact exist.

While I don't doubt that the screens Mrs R was being shown of her investment would've been realistic in appearance, I think Mrs R ought to have been cautious from the profits she appeared to be making – the value of her wallet appearing to be over $164,000 by September 2023. While Mrs R initially invested a more moderate sum of £2,000, she invested notably more just days later, which I think suggests the returns she was seeing were promising in a short time.

As the scam evolved into recovery firms contacting her, Mrs R again appears to have done limited research to ensure these firm's legitimacy. While she questioned whether she was being scammed, she proceeded to make payments, largely on the fraudster's word that this wasn't the case. In terms of the recovery scams, the first scam occurred as Mrs R received an unsolicited email referencing concerns she had been scammed, despite Mrs R not having raised these herself with anyone. When Mrs R fell victim to the second recovery scam, she enlisted a 'firm' who asked Mrs R again to pay fees up front (in cryptocurrency) before her compensation could be provided. I think as Mrs R was aware by this time of the existence of these scams, she ought to have shown more caution when researching a company to support her from the scam.

I therefore think there was enough going on during the scam that Mrs R ought also to have had concerns about whether the investment opportunity (and subsequent offers to recover her losses) were legitimate, and that she should have proceeded with more caution than she did as a result. I therefore think it's fair for Mrs R to be held partly responsible for her losses.

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

I've also thought about whether Revolut could have done more to recover the funds after Mrs R reported the fraud.

All but one of the payments were made by card to a cryptocurrency provider and that cryptocurrency was sent on 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 the cryptocurrency platform performed its given role in providing cryptocurrency in return for payment in sterling.

For the remaining payment transfer, as months had elapsed between this payment and the scam being raised with Revolut, I don't think Revolut would have had any prospects of recovering these funds from the beneficiary bank account.

Putting things right

I have provisionally decided that Mrs R's other banking provider should be held partially liable for £72,387.08 that was transferred from her account to Revolut, then on to the fraudsters, with her other banking provider refunding 33% of these losses.

As I think Revolut could also have stopped these same losses, I provisionally think that Revolut should also be held responsible for 33% of this sum lost (with Mrs R being responsible for the remaining 34%). Therefore Revolut should reimburse £23,887.74 of the first £72,387.08 Mrs R lost to the scam (from payment two onwards).

However, in addition to this, there was also a further £10,398.81 lost from Mrs R's Revolut account that was not transferred in from her other account referenced above. I therefore think liability for these further losses should be split 50/50 between Revolut and Mrs R, with Revolut reimbursing Mrs R £5,199.40.

My provisional decision

My provisional decision is that I partially uphold Mrs R's complaint against Revolut Ltd and consider that Revolut should reimburse Mrs R:

- *£29,087.14 of her losses incurred from the scam, as calculated above;*
- *8% simple interest from the date of these payments until the date of settlement.*

Mrs R accepted my provisional decision. Revolut confirmed it had nothing further to add and would await the final decision to proceed.

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.

As neither party has provided any new evidence that would otherwise change my opinion set out in the provisional decision, the outcome I've reached remains the same.

My final decision

My final decision is that I partially uphold Mrs R's complaint against Revolut Ltd and I direct Revolut to reimburse Mrs R:

- £29,087.14 of her losses incurred from the scam;
- 8% simple interest from the date of these payments until the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs R to accept or reject my decision before 11 June 2025.

Kirsty Upton
Ombudsman