DRN-4445613

The complaint

Mr R complains Revolut Ltd ("Revolut") didn't do enough to protect him when he fell victim to a scam.

What happened

Mr R said he saw an advertisement for an investment opportunity on social media which piqued his interest in part due to its professional nature and apparent celebrity endorsement, so he made enquiries in around February 2023. He said he found the website to be professional and carried the hallmarks of a legitimate company. He did some research and found positive reviews online and so decided to make further enquiries about the opportunity.

Mr R said he was contacted by an account manager, who I'll refer to as the scammer, that explained the opportunity further and was able to answer all questions and queries Mr R had in relation to the investment opportunity. He said they carried out verification checks requesting ID and proof of address for Mr R which he felt added legitimacy to the opportunity. He said they built a trusting relationship and he found them to be experienced in finances and their conduct to be professional. Mr R decided to invest with the scammer.

He said the scammer told him to open an account on their website and instructed Mr R to install remote access software which allowed the scammer to trade on his behalf. Mr R said the scammer had control of his device and showed him the trading portal which he was impressed by due to its detail and technical nature and it further reassured him of the legitimacy of the opportunity. The scammer gave him his login credentials and directed him to open an account with a cryptocurrency provider.

Mr R told us the scammer told him the first deposit needed to be £250 which Mr R made from an account not with Revolut. In March 2023 the scammer directed him to open an account with Revolut, from which the remaining payments towards the scam were made. The scammer assisted in opening the account by taking control of Mr R's device.

Below are the payments I find to be relevant to this complaint.

Payment	Date	Type of transaction	Payee	Amount
1	1 March 2023	Card payment	Cryptocurrency provider	£500
2	8 March 2023	Card payment	Cryptocurrency provider	£1,000
3	14 March 2023	Card payment	Cryptocurrency provider	£1,000
4	15 March 2023	Card payment	Cryptocurrency provider	£1,000
5	23 March 2023	Card payment	Cryptocurrency provider	£1,000
6	29 March 2023	Card payment	Cryptocurrency provider	£1,400
7	30 March 2023	Card payment	Cryptocurrency provider	£3,004.71
			Total loss	£8,904.71

Mr R said once he'd decided he was happy with his returns he notified the scammer who said he needed to make a further payment for insurance before withdrawal was possible. He did this.

Mr R explained he was contacted by another scammer related to this scam who informed him another company processed withdrawals, and it required a payment equal to 25% of the total profits. Mr R said he was hesitant and raised his concerns with the scammer who offered enough reassurance that Mr R made the payment as instructed. He said he was contacted again and told a further payment was needed before withdrawal was possible and when he challenged this the scammer became aggressive. At this time, he realised he'd been scammed.

Mr R contacted Revolut as he felt it hadn't done enough to protect him from losing his money to the scam. Revolut didn't uphold his complaint so he referred the matter to us. One of our Investigators considered the complaint and upheld it in part. They said Revolut ought to have intervened on the final payment and if it had it would've alerted Mr R to the scam, and he wouldn't have made the payment. They held Mr R jointly liable for the loss and recommended Revolut refund half of the final payment with 8% simple interest applied from the date of the loss until the date of settlement.

Mr R didn't accept the outcome. His representative said it felt Revolut ought to have done more to prevent Mr R making payments to a cryptocurrency provider and that a 50% deduction to his refund was unfair.

Revolut didn't agree with our Investigator's assessment, in addition to the points it made in its original submissions, in summary it said:

- There are no legal obligations, regulatory obligations, industry guidance, standards or codes of practice that apply to Revolut that oblige it to refund victims of authorised push payment ("APP") fraud. By suggesting that it does need to reimburse customers, it says our service is erring in law.

- The Payment Service Regulator's ("PSR") mandatory reimbursement scheme will not require it to refund payments where the victim has ignored warnings with gross negligence. Mr R was grossly negligent and failed to carry out sufficient due diligence.

- It would not be required to reimburse 'self-to-self' transactions even if it were a signatory to the Lending Standards Board's Contingent Reimbursement Model Code ("CRM Code"). Our service appears to be treating Revolut as if it were a signatory to the CRM Code.

- 'Self-to-self' payments don't meet either the Dispute Resolution Rules ("DISP Rules") or CRM Code definition of an APP scam.

As an agreement couldn't be reached the complaint has been passed to me for a decision.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

In broad terms, the starting position at law is that an Electronic Money Institution ("EMI") such as Revolut is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

And, as the Supreme Court has 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 Mr 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 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 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 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)[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

[1] For example, Revolut's website explains it launched an automated anti-fraud system in August 2018: https://www.revolut.com/news/revolut_unveils_new_fleet_of_machine_learning_technology_that_has_seen_a_fourfold_reduction_in_card_fraud_and_had_offers_from_banks_/

[2] Since 31 July 2023 under the FCA's new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.

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

involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).

- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

- The main card networks, Visa and Mastercard, don't allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain restrictions on their card issuers' right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of transaction, such as by location. The network rules did not, however, prevent card issuers from declining particular payment instructions from a customer, based on a perceived risk of fraud that arose from that customer's pattern of usage. So it was open to Revolut to decline card payments where it suspected fraud, as indeed Revolut does in practice (see above).

Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in 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.

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 Mr R was at risk of financial harm from fraud?

It isn't in dispute that Mr R has fallen victim to a cruel scam here, nor that he authorised the payments he made by transfers to his cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

Whilst I have set out in some detail in this decision the circumstances which led Mr R to make the payments using his Revolut account and the process by which that money ultimately fell into the hands of the scammer, 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 Mr 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 all payments would be credited to a cryptocurrency wallet held in Mr R's name.

By March 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[4]. And by March 2023, when these payments took place, further restrictions were in place[5]. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

I recognise that, as a result of the actions of other payment service providers, many customers who wish to purchase cryptocurrency for legitimate purposes will be more likely to use the services of an EMI, such as Revolut. And I'm also mindful that a significant majority of cryptocurrency purchases made using a Revolut account will be legitimate and not related to any kind of fraud (as Revolut has told our service). However, our service has also seen numerous examples of consumers being directed by fraudsters to use Revolut accounts in order to facilitate the movement of the victim's money from their high street bank account to a cryptocurrency provider, a fact that Revolut is aware of.

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mr R made in 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.

---

[4] See for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022. NatWest Group, Barclays, Lloyds Banking Group and Santander had all introduced some restrictions on specific cryptocurrency exchanges by August 2021

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

To be clear, I'm not suggesting as Revolut argues 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 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.

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

I think Revolut should have identified that payments 1 to 6 were going to a cryptocurrency provider (the merchant is a well-known cryptocurrency provider), but they were low in value and made over several weeks, and I don't think Revolut should reasonably have suspected that they might be part of a scam.

However, payment 7 was larger in value (at more than twice that of Payment 6). Given what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Mr 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 Mr 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. Instead, as I've explained, I think it was a combination of the characteristics of this payment (combined with those which came before it, and the fact the payment went to a cryptocurrency provider) which ought to have prompted a warning.

Revolut argues that it is unlike high street banks in that it provides cryptocurrency services in addition to its electronic money services. It says that asking it to 'throttle' or apply significant friction to cryptocurrency transactions made through third-party cryptocurrency platforms might amount to anti-competitive behaviour by restricting the choice of its customers to use competitors. As I have explained, I do not suggest that Revolut should apply significant friction to every payment its customers make to cryptocurrency providers. However, for the reasons I've set out above I'm satisfied that by March 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.

What did Revolut do to warn Mr R?

Revolut told us there was no intervention on any of the payments Mr R made. It said the first contact it had with Mr R was when he reported the scam.

What kind of warning should Revolut have provided?

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

Taking that into account, I think Revolut ought, when Mr R attempted to make payment 7, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency scam, without significantly losing impact.

So, at this point in time, I think that such a warning should have addressed the key risks and features of the most common cryptocurrency scams – cryptocurrency investment scams. The warning Revolut ought fairly and reasonably to have provided should have highlighted, in clear and understandable terms, the key features of common cryptocurrency investment scams, for example referring to: an advertisement on social media, promoted by a celebrity or public figure; 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 Mr 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.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr R suffered from payment 7?

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 Mr R's payments, such as finding the investment through a social media advertisement endorsed by a celebrity, being assisted by a broker and being asked to download remote access software so they could help him open cryptocurrency wallets.

Overall, I think that a warning provided by Revolut would have given the perspective Mr R needed. I don't have the correspondence or conversations to review between Mr R and the scammer. I've had no evidence or testimony that Mr R was given a cover story and nothing to suggest he was told to, or would agreed to, disregard any warning provided by Revolut. I've also seen no indication that Mr R expressed mistrust of Revolut or financial firms in general. Or that he was so taken by the scammers that he would disregard a tailored investment warning like the one described above.

Mr R topped-up his account at Revolut using another of his accounts with a high street bank, which has confirmed it gave no warnings regarding the payments he made to Revolut. Meaning Mr R wasn't on notice to the possibility he might be falling victim to a scam. It's important to note Revolut knew payment 7 was identifiably going to a cryptocurrency platform. Something the sending bank is not as likely to have known.

Therefore, on the balance of probabilities, had Revolut provided Mr R with an impactful warning that gave details about cryptocurrency investment scams and how he could protect himself from the risk of fraud, I believe it would have resonated with him. He could have paused and looked more closely into the broker before proceeding, as well as making further enquiries into cryptocurrency scams and whether or not the broker was regulated in the UK or abroad. I'm satisfied that a timely warning to Mr R from Revolut, would very likely have caused him to stop and carry out further research – revealing the scam and preventing his further losses.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr R purchased cryptocurrency which credited an e-wallet held in his own name, rather than making a payment directly to the scammers. So, he remained in control of his money after he made the payments from his Revolut account, and it took further steps before the money was lost to the scammers.

I have carefully considered Revolut's view that in a multi-stage fraud, a complaint should be properly considered only against either the firm that is a) the 'point of loss' – the last point at which the money (or cryptocurrency) remains under the victim's control; or b) the origin of the funds – that is the account in which the funds were prior to the scam commencing. It says it is (in this case and others) merely an intermediate link – being neither the origin of the funds nor the point of loss and it is therefore irrational to hold it responsible for any loss.

In reaching my decision, I have taken into account that the Final Payment was made to another financial business (a cryptocurrency exchange) and that the payments that funded the scam were made from other accounts at regulated financial businesses.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr R might have been at risk of financial harm from fraud when he made payment 7, 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 he 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 Mr R's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr 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.

I've also considered that Mr R 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 Mr R could instead, or in addition, have sought to complain against those firms. But Mr R has not chosen to do that and ultimately, I cannot compel him to. In those circumstances, I can only make an award against Revolut.
I'm also not persuaded it would be fair to reduce a consumer's compensation in circumstances where: the consumer has only complained to us 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 Mr R's loss from payment 7 (subject to a deduction for Mr R's own contribution which I will consider below).

Should Mr R bear any responsibility for their 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.

I recognise that, as a layman who claims to have little investment experience, there were aspects to the scam that would have appeared convincing. Mr R was introduced to it through an advert appearing to be endorsed by a celebrity. I haven't seen this particular advert, but I've seen other examples. In my experience, they often appear as paid adverts on social media websites and a reasonable person might expect such adverts 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 scammers used the apparent success of early trades and, as in this case, the appearance of a small investment to begin with. I can understand how what might have seemed like taking a chance with a relatively small sum of money snowballed into losing a life changing amount of money.

So I've taken all of that into account when deciding whether it would be fair for the reimbursement due to Mr R to be reduced. I think it should.

Mr R says he carried out checks into the investment company prior to investing, like internet searches, and I'm persuaded he did do some research.

From Mr R's testimony I'm persuaded he had his doubts prior to making payment 7. He said he was hesitant and raised concerns with the scammer when he was asked to pay a fee before he could make a withdrawal. And I've seen evidence from the sending bank that Mr R's testimony when reporting the scam to it, was that he discussed things with his wife prior to payment 7 and she advised he shouldn't make the payment.

While I appreciate that Mr R's difficulty withdrawing funds was what alerted him to the scam, I'm persuaded he had suspicions which ought reasonably to have caused him to have concerns about whether the investment was genuine before payment 7 was made from his Revolut account.

For the avoidance of doubt, it is not my finding that Mr R knew that he was likely falling victim to a scam and went ahead anyway. Rather my finding is that he seems – to some extent – to have been suspicious that the investment opportunity was a scam.

I've concluded, on balance, that Revolut can fairly reduce the amount it pays to Mr R because of his role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

I recognise that Mr R did have a role to play in what happened, and it could be argued that he should have had greater awareness than he did that there may be something suspicious about the investment scam. But I have to balance that against the role that Revolut, an EMI subject to a range of regulatory and other standards, played in failing to intervene. Mr R was taken in by a cruel scam – he was tricked into a course of action by a scammer and his actions must be seen in that light. I do not think it would be fair to suggest that he is mostly to blame for what happened, taking into account Revolut's failure to recognise the risk that

he was at financial harm from fraud, and given the extent to which I am satisfied that a business in Revolut's position should have been familiar with a fraud of this type. Overall, I remain satisfied that 50% is a fair deduction to the amount reimbursed in all the circumstances of the complaint.

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

I've also thought about whether Revolut could have done more to recover the funds after Mr R reported the fraud and I've considered whether Revolut took the steps it should have once it was aware that the payments were the result of fraud.

The payments were sent to a known cryptocurrency exchange. In that case the money would have been exchanged into cryptocurrency and sent on to the wallet Mr R gave, this was supplied to him by the scammer. It seems that Mr R got the cryptocurrency he paid for and in these cases, there's no real prospect of successful recovery of funds.

Putting things right

As outlined above, Revolut could have prevented a £3,004.71 payment to the scam. Revolut should now refund this payment less 50% because of Mr R's contributory negligence. I find this is fair and reasonable for the reasons I have explained above.

My final decision

For the reasons given above, I uphold this complaint in part and direct Revolut Ltd to pay Mr R:

- 50% of payment 7 which I calculate to be £1,502.36
- Pay 8% simple interest per year on this amount, from the date the payment debited his account, until the date the refund is settled (less any tax lawfully deductible)

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr R to accept or reject my decision before 5 March 2025.

Charlotte Mulvihill
Ombudsman