

The complaint

Mr L complains that Revolut Ltd has declined to refund payments he made as part of an investment scam.

What happened

While Mr L has a representative in bringing this complaint – for simplicity I’ll refer to Mr L in relation to comments made by him and on his behalf.

Mr L says that he saw a celebrity advertising a method of investing in cryptocurrency on social media. He then completed a form and provided his contact details on a professional looking website. Following this Mr L was contacted by the scammers purporting to be financial advisers who requested an initial sign-up fee. Mr L was instructed to download remote access software so that he could be shown how to trade. As part of the scam Mr L was given log in details to a platform which appeared to show live trades and profits. To fund his trading account, Mr L was advised that he’d need to purchase cryptocurrency from a legitimate cryptocurrency provider. Mr L was also asked to send funds to individuals who he understood to be the scammer’s colleagues.

Mr L opened an account with Revolut on 30 March 2023 and funded it with payments from his main account with Bank A. Mr L spoke to Bank A three times on the 30 March 2023, and in one of the calls Mr L was asked about the reason for the payment of £2,500 to Revolut. Mr L said it was to “diversify his funds”, he also confirmed he had opened the Revolut account, hadn’t been contacted by a bank or financial service to make the payment, and hadn’t been asked to lie, he hadn’t been told his money was unsafe, he didn’t have remote access software. He was then given a warning about safe account scams.

Once funds were available in Mr L’s Revolut account, he made the below payments from his Revolut account. Payment 1 went to a merchant providing educational services, and payments 2, 3, and 6 are all to a well-known crypto currency platform and the transfers are to third parties. Mr L was then told he needed to pay a 9% broker fee to withdraw his profits and the payments on 21 April 2023 relate to that.

Payment number	Date	Payment type	Amount
1	30 March 2023	Card payment	£425
2	30 March 2023	Card payment	£2,990
3	7 April 2023	Card payment	£2,990
4	7 April 2023	Transfer	£9,000
5	21 April 2023	Transfer	£16,000
6	21 April 2023	Card Payment	£1,540

When Mr L reported the scam to Revolut Ltd, it declined to provide a refund on the basis that the payments were authorised. It said it had declined payments 4 and 5 when they were first attempted and provided sufficient warnings before Mr L proceeded to make them. It also said the card payments were money orders and so a chargeback wouldn't have been successful.

Mr L referred the matter to our service and said Revolut should have done more to intervene and provide effective warnings.

Revolut, in its submissions to our service argued it was not liable for the following reasons:

- All transfers and card payments were initiated and authorised by Mr L.
- Part of the fraudulent activity did not take place on the Revolut platform. Revolut was used as an intermediary to receive funds from Mr L's main bank account and then transferred on to his legitimate external account held with a cryptocurrency platform. Mr L subsequently lost control of the funds further in the chain.
- Proportionate and appropriate scam warnings were displayed to Mr L.
- Unrealistic returns were not questioned by Mr L.
- Mr L's lack of appropriate due diligence.
- The scam was not a 'heat of the moment' single payment or 'out of character transaction scenario but an investment scam where payments were sent over a period of 22 days.

When Mr L brought the complaint to our service, the investigator didn't uphold it. In summary they thought Revolut ought to have done more to intervene at payment four, but they weren't persuaded a proportionate intervention would have identified the scam Mr L had fallen victim to. So, they didn't think it was likely Revolut could have prevented Mr L's loss.

Mr L didn't agree, he said he was honest during Bank A's intervention and that he hadn't downloaded remote access software until later. And that the focus of that call had been questions related to a safe account scam. Mr L told Bank A that the purpose of the payment was to "*diversify his money*" and that if he'd been asked more probing questions this would have revealed the scam as he hadn't been told to lie or given a cover story. Mr L says this would also have been the case had Revolut asked him specific and probing questions.

As no agreement could be reached, the case was passed to me to decide. I issued my provisional decision on 13 March 2025; here I explained why I intended on upholding the complaint. I also said that the settlement I intended to award was dependent on further evidence of loss. This has since been provided by Mr L and shared with Revolut.

No response has been received from Revolut, despite follow up emails from our service. As the deadlines set have now passed, the matter has been passed back to me for a final 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.

Having done so I'm upholding this complaint, I'll explain why.

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 L 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 / April 2023 have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

In reaching the view that Revolut should have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances, I am mindful that in practice all banks and EMI's like Revolut did in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;¹
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system for authorised push payments;
- providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified.

For example, it is my understanding that in March / April 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat).

I am also mindful that:

- 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".

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.

- 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 Code³, which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).
- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.
- The main card networks, Visa and Mastercard, don't allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain restrictions on their card issuers' right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of transaction, such as by location. The network rules did not, however, prevent card 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 / April 2023 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;

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

- 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 / April 2023, Revolut should in any event have taken these steps.

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

It isn't in dispute that Mr L has fallen victim to a cruel scam here, nor that he authorised the disputed payments he made to his cryptocurrency wallet (from where his funds were subsequently transferred to the scammer). Mr L also authorised the payments transferred to third party accounts.

Whilst I have set out the circumstances which led Mr L to make the payments using his Revolut account and the process by which that money ultimately fell into the hands of the fraudster, I am mindful that Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Mr L might be the victim of a scam.

I'm aware that cryptocurrency exchanges like the one Mr L paid 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 have been aware of this fact.

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 transactions⁴. And by March 2023, further restrictions were in place⁵.

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.

This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

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

So, taking into account all of the above I'm satisfied that by the end of 2022, prior to the payments Mr L 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 Mr L'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 L might be at a heightened risk of fraud that merited its intervention.

Should Revolut have identified that Mr L might be at a heightened risk of fraud?

I'm conscious that Mr L opened his account with Revolut on 30 March 2023 and so there was no account history to compare the activity to. Mr L then credited the account to fund the disputed payments. On the same day an initial payment was reverted before payments one and two (from the table above) were successfully processed.

Payment two was for £2,990 and Revolut knew or ought to have known the payment was going to a cryptocurrency provider. I explained above why by March 2023 I think Revolut I should have recognised that payments to cryptocurrency carried a higher risk of being associated with fraud.

Bearing in mind the pattern of activity on a newly opened account and the value of this payment being just below £3,000 when a payment had already been made that day, I think Revolut should have recognised there was a heightened possibility that the transaction was linked to a cryptocurrency scam, and this should have prompted an intervention from Revolut before it was processed.

What kind of warning should Revolut have provided?

As I've said, I think Revolut ought to have identified the heightened risk that Mr L was making payment 2 in relation to a cryptocurrency scam. In line with the good industry practice that I've set out above, I think Revolut should have provided a specific, tailored and impactful warning before processing it.

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 L attempted to make payment 2, 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 L by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

What did Revolut do to warn Mr L?

Here Revolut didn't intervene in payments one, two or three. But when Mr L set up a new payee for payments four and five, he received a new payee warning that said:

"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".

Payment four and five were also declined and Mr L was shown a warning that said:

"Our systems have identified your transaction as highly suspicious. We declined it to protect you. If you decide to make the payment again anyway, you can, and we won't decline it. As we have warned you this transaction is highly suspicious and not to make the payment, if the person you pay turns out to be a fraudster, you may lose all your money and never get it back." Mr L was also given a link to more information on scams.

If Revolut had provided a warning of the type described, would that have prevented the losses Mr L suffered from payment 2 onwards?

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 L's payments, such as finding the investment through an advertisement endorsed by a public figure, being assisted by an intermediary and being asked to download remote access software so they could help him trade.

I've seen no indication that Mr L expressed mistrust of Revolut – Mr L says the scammer told him that banks might try to stop him making payments but based on the fact Mr L was asked to send money to a cryptocurrency platform via Revolut this was likely in relation to Bank A. And I don't think this alone would have prevented Mr L from taking a warning seriously that resonated closely with what he was doing.

I haven't seen anything to suggest that Mr L developed a personal or romantic relationship with the scammer rather than a professional one. And given it would have been very early on in the scam I don't think a strong relationship of trust had been established yet which would have impacted the effectiveness of a relevant warning. Nor had Mr L seen any fictitious trading and profits at this time.

While Mr L did receive some intervention from Bank A, and from Revolut later on, none of the warnings he received were specific to an investment or cryptocurrency scams. And so, I don't think the fact he continued to make payments on those occasions is indicative of how he would have responded to a relevant warning at payment 2.

Therefore, on the balance of probabilities, had Revolut provided Mr L 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 financial advisers / broker before proceeding, as well as making further enquiries into cryptocurrency scams. I note that if Mr L had searched for the financial adviser's company online at the time he would have found negative Trust Pilot reviews about it being a scam.

So, I'm satisfied that had Revolut provided an appropriate warning, it's likely Mr L would've recognised many of these features applied to his own situation and the warnings would have resonated with him. In the circumstances, I think he'd have ultimately chosen not to proceed with the payment.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Mr L made some of the payments using his Revolut account to another account in his own name, rather than directly to the fraudster, so he remained in control of his money after he made the payments, and there were further steps before the money was lost to the scammer.

Mr L has provided evidence of loss from his account with the cryptocurrency platform, so for the reasons I have set out above, I am satisfied that it is fair to hold Revolut responsible for Mr L's losses from payment 2, subject to a deduction for Mr L's own contribution towards his loss.

As I have 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.

But as I've set out in some detail above, I think that Revolut still should have recognised that consumer might have been at risk of financial harm from fraud when they made payment 2, 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 Mr L 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 L's own account does not alter that fact and I think Revolut can fairly be held responsible for Mr L'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 L 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 L could instead, or in addition, have sought to complain against those firms. But Mr L 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 Mr L's compensation in circumstances where: the Mr L has only complained about one respondent from which they are entitled to recover their losses in full; Mr L 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 L's loss from payment 2 (subject to a deduction for his own contribution which I will address below).

Should Mr L 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 L was introduced to it through an advert appearing to show a well-known media personality being interviewed on a popular television programme. 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 fraudsters used the apparent success of early trades and, as in this case, the apparent ability to withdraw funds to encourage increasingly large deposits. 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 L to be reduced. I think it should.

Mr L appears to have undertaken very limited research before he invested, however that fact alone wouldn't necessarily be enough for me to consider that there should be a deduction to the amount awarded. But I'm concerned by the plausibility of the returns versus risk that he thought were present in this investment opportunity.

Mr L appeared to be under the impression that he could make a significant amount of money in a very short space of time with little to no risk. Specifically, Mr L told Revolut that on 7 April 2023 he decided to invest further because he was promised that *“in 10 days we would sell ... silly price at a ridiculous profit”* and *“it’s a no loss situation its 1 million per cent win win”*. And that on the 18 April 2023 he was told *“the profits are going to be around 173,000 pounds”* – it was on this basis that he decided to pay a broker’s fee of 9% which he initially challenged as this hadn’t been mentioned before he invested. I think this should have sounded too good to be true to Mr L and affected the overall plausibility of the scam, putting him on notice that it might not be genuine. I understand Mr L says he didn’t know these kinds of profits were unrealistic, but I think his choice of language demonstrates an awareness that this is an unusual level of profit.

I’ve concluded, on balance, that Revolut can fairly reduce the amount it pays to Mr L because of his role in what happened. Weighing the fault that I’ve found on both sides, I think a fair deduction to make from payment 3 is 50%.

I don’t, however, think a reduction would be fair to apply to payment 2 because it was Mr L’s first payment towards the investment and the issues I’ve explained above in relation to the plausibility of the scam are relevant from when Mr L was persuaded to invest further on 7 April 2023.

Could Revolut have done anything else to recover Mr L’s money?

I’ve also thought about whether Revolut could have done more to recover the funds after Mr L reported the fraud. Payment 1 was made to a merchant and payments 2, 3, and 6 were card payments to the cryptocurrency platform. I’m not persuaded there would have been any reasonable prospect for a chargeback claim succeeding, as the merchant would likely be able to demonstrate that it had provided the goods/services that had been purchased.

Payments 3 and 4 were faster payments to a third-party account held outside of the UK. We’re aware that the receiving account provider was not returning funds to the sending account when requested on the basis of suspected fraud at the time.

So, for the reasons explained, I don’t think there was anything more Revolut could’ve done to recover the money in these circumstances.

Putting things right

The principal aim of any award I make must be to return Mr L to the position he’d now be in but for the errors or inappropriate actions of Revolut, while allowing for any responsibility he should reasonably bear.

If Revolut had carried out an appropriate intervention as I’ve described, I’m satisfied the scam would have been stopped at payment 2 and Mr L would have retained the money that was lost.

I’m conscious Mr L has described borrowing money from his mother to fund payments 5 and 6 and so while I understand he has or will need to pay that money back, I’m not aware he is paying any interest on that borrowing. So, I’ll take that into account when making my award.

Mr L has now provided evidence of loss from his cryptocurrency account, and this has been shared with Revolut and so I think it is fair to include payments to this platform in my award.

My final decision

For the reasons I've explained, I uphold this complaint and require Revolut Ltd to do the following to put things right.

1. Pay Mr L 100% of payment 2.
2. Pay Mr L 50% of payments 3 and 4.
3. Pay Mr L 50% of payments 5 and 6.
4. Pay Mr L simple interest on the amount in points 1 and 2, at a rate of 8% per year from the date of the payments to the date of settlement.

Interest is intended to compensate Mr L for the period he was unable to use this money. If HM Revenue & Customs (HMRC) requires Revolut to deduct tax from any interest, Revolut must provide Mr L with a certificate showing how much tax has been deducted if he asks for one. I'm satisfied this represents a fair and reasonable settlement of this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr L to accept or reject my decision before 28 April 2025.

Stephanie Mitchell
Ombudsman