DRN-5091120

The complaint

Mrs H complains Revolut Ltd ("Revolut") didn't do enough to protect her when she fell victim to a scam.

What happened

Mrs H said in January 2023 she saw an advert on social media regarding a cryptocurrency investment opportunity. She clicked the link, entered her details, and was later contacted by an 'account manager' who'll I'll refer to as the scammer. She said they were professional and knowledgeable. She said she carried out research which was positive and Mrs H decided to go ahead with the opportunity.

Mrs H said the scammer informed her they'd be trading on her behalf and provided a username and password for an account. And she was directed to open a Revolut account as high street banks did not like customers trading in cryptocurrency.

Mrs H told us she made an initial investment of £250 from an account other than Revolut, after which the scammer started to contact her regularly each week. They suggested showing Mrs H the withdrawal process and she was able to make a minimal withdrawal of £79.54. Mrs H said the above gave her confidence in the legitimacy of the investment opportunity and she invested larger sums.

In March 2023 Mrs H said she was informed by the scammer that her profits had 'crashed' and she should invest further to recoup her funds which she did. It's at this time she was told to install remote access software.

When her further investments didn't result in a positive return into her account, Mrs H realised she had been scammed.

Below are the transactions I find to be relevant:

Payment	Date	Type of transaction	Payee	Amount
	18 January 2023	Credit		£79.54
1	**23 January 2023**	**Card payment**	**Cryptocurrency provider**	**£1,000**
2	**8 February 2023**	**Card payment**	**Cryptocurrency provider**	**£5,000**
3	**8 February 2023**	**Card payment**	**Cryptocurrency provider**	**£3,000**
	20 February 2023	Credit		£825.86
4	**23 March 2023**	**Card payment**	**Cryptocurrency provider**	**£2,000**
5	**30 March 2023**	**Card payment**	**Cryptocurrency provider**	**£1,000**
6	**4 April 2023**	**Card payment**	**Cryptocurrency provider**	**£2,000**

Unhappy with Revolut's response, Mrs H raised the matter with the Financial Ombudsman. One of our Investigators looked into the complaint and upheld it in part. They said Revolut should refund the money lost from payment 3 onwards, less Mrs H's credits. They held Mrs H and Revolut equally liable for the loss meaning she should receive half of the funds back.

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

- 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.

- It is an intermediary in the chain of the scam as the source of the funds lost to this scam originated from a firm other than Revolut. It said the Financial Ombudsman should consider the actions of other firms in the chain.

As an agreement could not be reached, the complaint has been passed 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.

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 H 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 January 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 January 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and

[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_/

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 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

[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"

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

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

It isn't in dispute that Mrs H has fallen victim to a cruel scam here, nor that she authorised the payments she made to her cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

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

I've considered what Revolut knew about the payments when it received Mrs H's payment instructions and I'm satisfied Revolut ought to have known they were all going to a known cryptocurrency provider. 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 the disputed payments would be credited to a cryptocurrency wallet held in Mrs H's name.

By January 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 January 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 Mrs H made in January 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

To be clear, I'm not suggesting as Revolut 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 January 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 most of the payments in this

---

[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.

case were going to an account held in Mrs H's own name should have led Revolut to believe there wasn't a risk of fraud.

So I've gone onto consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Mrs H might be at a heightened risk of fraud that merited its intervention.

As mentioned, Revolut should have identified that all the payments Mrs H made from her Revolut account towards the scam were going to a cryptocurrency provider (the merchant is a well-known cryptocurrency provider). I don't think it ought to have been concerned about payment 1 as it was relatively low in value and I don't think Revolut should reasonably have suspected that it might be part of a scam or that Mrs H was at risk of financial harm from fraud. So, I can't say Revolut was at fault for processing payment 1 in accordance with Mrs H's instructions.

I'm persuaded that Revolut ought to have been concerned by payment 2. At the time the payment was made, I think it was reasonable for Revolut to take into account a range of factors when deciding whether to make further enquiries of its customer about a particular payment. But I'm also taking into account that scams involving cryptocurrency were becoming increasingly prevalent and well-known at that time. Payment 2 was for a significantly higher amount than payment 1 and was going to a known cryptocurrency provider. On balance, taking into account that Revolut needs to take an appropriate line between protecting against fraud and not unduly hindering legitimate transactions, and also considering the value of this payment, I think Revolut ought to have been sufficiently concerned about this payment and it would have been fair and reasonable to expect it to have provided a warning to Mrs H at this point.

I also note payment 3 was made only two minutes after payment 2 and given what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Mrs H 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 its customer 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 these payments (combined with that which came before it, and the fact the payments went to a cryptocurrency provider) which ought to have prompted a warning for both payments 2 and 3. I'll come on to later what I expect proportionate warnings to be.

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 January 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 Mrs H?

Revolut hasn't told us it gave any warnings to Mrs H, it said it had no reason to suspect the payments may have been fraud related.

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 payments 2 and 3 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 Mrs H attempted to make payment 2, knowing it was going to a cryptocurrency provider, to have provided a written warning that was specifically about the risk of cryptocurrency investment 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 scams, 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 Mrs H by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk that payment 2 presented.

As mentioned, payment 3 was made two minutes after payment 2 and overall, I'm satisfied that Revolut should have identified payment 3 as carrying a heightened risk of financial harm and should have taken additional steps before allowing it to debit Mrs H's account.

Having thought carefully about the risk payment 3 presented, I think a proportionate response to that risk would be for Revolut to have attempted to establish the circumstances surrounding the payment before processing the payment. I think it should have done this by, for example, directing Mrs H to its in-app chat to discuss the payment further.

If Revolut had provided warnings of the type described, would that have prevented the losses Mrs H suffered from payment 2?

I've considered if a cryptocurrency scam warning as described above would likely have positively impacted Mrs H and stopped her from making payment 2, and I'm not persuaded it would have done.

Mrs H transferred funds into her Revolut account from another account she held with a high street bank. I've seen evidence that bank held a payment for £8,000 and there was an intervention call. I've listened to that call and when asked why she was transferring the funds from her account to Revolut Mrs H says it's being paid into a savings account with a higher rate as she's saving for a holiday. The bank enquires further about this, and Mrs H is reluctant to provide more details and notes she is in a rush and says the call is long.

We know Mrs H wasn't transferring the money to save for a holiday but to invest in cryptocurrency. Her testimony on why she didn't give the sending bank the full details of her intensions Mrs H said she had been told by the scammer not to speak with any banks or the cryptocurrency provider. There's no indication Mrs H was being actively guided through this call or that she was given a cover story.

Because of the above I think had Revolut intervened in the way I've described; I think it's unlikely the warning would have positively impacted Mrs H and prevented her from making the payment. Given that Mrs H appeared to be following the advice the scammer had given her previously, and that an earlier intervention with the sending bank hadn't resonated with her, I'm not persuaded that a written warning would ultimately have prevented her from making payment 2.

Given payment 3 was made so soon after payment 2 I think it represented an increase in the risk that Mrs H was at potential harm from fraud. And I think a proportionate response to that risk would have been for Revolut to have gone beyond a written warning. In my view, it should have done more to establish the potential risk of this payment through a direct human intervention by one of its agents to discuss the situation in more detail (for example, through its in-app chat).

If Revolut had attempted to establish the potential risk through a human intervention, there would have been an opportunity for Revolut to find out more about the wider circumstances of the payment and to probe further on the answers Mrs H gave.

I'm mindful Mrs H wasn't forthcoming with the sending bank, and it could be argued she wouldn't have been with Revolut either. Although we know from Mrs H's testimony that she'd been directed to open a Revolut account as high street banks didn't like customer's trading in cryptocurrency. I think on balance this contributed to Mrs H's actions during the call with the sending bank. As she was of the belief Revolut allowed its customers to trade in cryptocurrency I believe she may have been more incline to be truthful with Revolut when compared with a high street bank.

Additionally, a key difference here is Revolut was aware (unlike the sending bank) that the payment was going to a cryptocurrency provider. So had a human intervention happened in the way I'd expect, the agent would have been able to probe Mrs H further and I think the cover story she decided to give the sending bank wouldn't have held up in the circumstances given the destination of the payment. And any additional untruths from Mrs H would have more likely than not raised suspicions with Revolut.

I think had Revolut carried out an effective human intervention asking open probing questions via the in-app chat it would have given Mrs H the perspective needed and ultimately, I believe on balance it would have prevented her from making payment 3 and those that followed.

Is it fair and reasonable for Revolut to be held responsible for the loss?

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

But as I've set out in some detail above, I think that Revolut still should have recognised that Mrs H might have been at risk of financial harm from fraud when she made payment 3, 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 Mrs H 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 Mrs H's own account does not alter that fact and I think Revolut can fairly be held responsible for Mrs H'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 Mrs H 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 Mrs H could instead, or in addition, have sought to complain against those firms. But Mrs H has not chosen to do that and ultimately, I cannot compel her to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mrs H's compensation in circumstances where: the consumer has only complained about one respondent from which they are entitled to recover their losses in full; has not complained against the other firm (and so is unlikely to recover any amounts apportioned to that firm); and where it is appropriate to hold a business such as Revolut responsible (that could have prevented the loss and is responsible for failing to do so). That isn't, to my mind, wrong in law or irrational but reflects the facts of the case and my view of the fair and reasonable position.

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be referred to me) and for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Mrs H's loss from payment 3 (subject to a deduction for Mrs H's own contribution which I will consider below).

Should Mrs H 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.

I recognise that, as a layperson with little investment experience, there were aspects to the scam that would have appeared convincing. Mrs H was introduced to it through an advert on social media. 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 Mrs H to be reduced. I think it should.

While I can't be certain, I think it's fair to conclude that had Mrs H been forthcoming with the sending bank the scam would have more likely than not been uncovered sooner and her losses prevented. In not doing so I think it is fair to reduce the settlement Mrs H receives and for her to share the liability for her losses with Revolut at 50%.

I recognise that Mrs H had a role to play in what happened, and it could be argued that she should have had greater awareness than she 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. Mrs H was taken in by a cruel scam – she was tricked into a course of action by a scammer and her actions must be seen in that light. I do not think it would be fair to suggest that she is mostly to blame for what happened, taking into account Revolut's failure to recognise the risk that she 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 Mrs H's money?

I've thought about whether there's anything else Revolut could have done to help Mrs H and I've considered whether Revolut took the steps it should have once it was aware that the payments were the result of fraud.

Mrs H's payments were to purchase cryptocurrency. In that case the money would have been exchanged into cryptocurrency and sent on to the wallet she gave, this was supplied to her by the scammer. It seems that Mrs H got the cryptocurrency she paid for and in these cases, there's no real prospect of successful recovery of funds.

Putting things right

Revolut could have prevented £8,000 from being lost to the scam. But I've seen evidence that after payment 3 was sent to the scam, Mrs H received a return of £825.86. So I've deducted this return from the loss I think Revolut could have prevented, leaving a total outstanding loss for payments 3 to 6 of £7,174.14.

My final decision

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

- 50% of her total outstanding loss for payments 3 to 6, £7,174.14, which I calculate to be £3,587.07.
- Pay 8% simple interest per year on this amount, from the date the payments debited her 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 Mrs H to accept or reject my decision before 8 May 2025.

Charlotte Mulvihill
Ombudsman