DRN-5034654

The complaint

Miss W complains that Revolut Ltd won't refund money she lost when she was the victim of a crypto investment scam.

Miss W is represented by a firm I'll refer to as 'C'.

What happened

The background to this complaint is well known to both parties and so I'll only refer to some key events here.

In 2023 Miss W saw an advert for online investing on a social media platform with a firm I'll refer to as 'AT', which we now know to be a scam. Miss W considered the advert extremely professional and was reassured by a feature on a financial information website ran by a well-known public figure endorsing AT. Unfortunately, Miss W was unaware that such a spoofing technique that was used here was possible.

Miss W followed the link and went to AT's website, whereby she was impressed with the detailed and technical nature of it. As an inexperienced investor, she carried out some checks online but didn't find any negative information. So, she was confident it was a genuine opportunity and completed AT's enquiry form.

AT contacted Miss W, whom she found professional and articulate, and assisted her – using remote desktop software – to set up a trading account with them and a wallet with a legitimate crypto exchange. Miss W made an initial $250 investment which she funded from another banking provider. But after seeing reasonable profits on this initial investment, AT persuaded her to invest more. And to do this, they advised Miss W to open a Revolut account that was dedicated specifically for this purpose.

Miss W made the following payments to AT's trading platform from her Revolut account via a legitimate crypto exchange:

Transaction date	Type of transaction	Amount
30 May 2023	Debit card	$1,100
31 May 2023	Debit card	£1,000
31 May 2023	Debit card	£1,500
6 June 2023	Debit card	$5,173
7 June 2023	Debit card	£3,000
	Total loss:	£5,500 + $6,273

The first three payments were for investment purposes. And as Miss W was happy with the profits visible on her AT trading account, she requested a withdrawal. At this point, the scammer told Miss W she had to pay a liquidity fee ($5,173) which was then followed by a requirement to pay tax (£3,000). Despite paying these, Miss W didn't receive the withdrawal funds and was told that she had to pay a further $7,000 as her profits had increased. At this

point, Miss W has explained that she spoke to a family member regarding borrowing funds, who carried out some further research and which led to her realising she'd been scammed.

Miss W reported the scam payments to Revolut on 12 June 2023. Revolut directed her to submit chargeback claims which were rejected.

C complained, on Miss W's behalf, to Revolut on 1 August 2023 saying the payments were made as part of a scam. In short, they said:

- Revolut failed in their duty of care to protect Miss W and prevent her loss.
- Newly opened accounts present a greater risk of misuse compared to established accounts.
- Revolut failed to intervene at any point or provide an effective warning – despite the payments being highly usual.
- Had Revolut flagged the payments for additional security and asked probing and open-ended questions, Miss W would've answered these openly and honestly. In turn, Revolut would've immediately been able to identify it was an investment scam. So, had Revolut blocked and investigated the payments as they should have, the payments and loss associated with them would've been prevented.
- Miss W had a reasonable basis to believe AT was genuine. This is because, amongst other reasons:
    - AT's website mirrored that of a legitimate business, they followed strict security polices and were knowledgeable and articulate.
    - The scammers were professional and used good business practice, such as scheduling appointments in advance.
    - The trading platform showed her investment balance making good returns on what she considered a secure account that only she had access to.
    - She carried out research but found little/no evidence of negative reviews.
- Miss W was vulnerable at the time of the scam due to ill-health, which made her less able to represent her own interests and it was something the scammer exploited.
- To settle this complaint, they said Miss W would accept full reimbursement of her losses, 8% interest and £300 compensation.

Revolut didn't uphold the complaint. In short, they said:

- The chargeback process is framed by a very detailed and consistent set of rules – dictated by the card scheme – which they're required to follow. The process includes two types of claims – fraud or dispute – with fraud claims raised for these transactions.
- The outcome of the claims was that they had no right to dispute them as they'd found no traces of fraudulent activity on Miss W's account – as the transactions were verified through an additional layer of security (3DS). So, they weren't valid chargebacks under the scheme rules, and they were required to reject them.
- They take fraud very seriously and have implemented security measures to minimise and prevent the chance for such events to take place. They also provide some preventative resources to their customers – such as articles on their website/blog.

The complaint was referred to the Financial Ombudsman. Our Investigator thought it should be upheld in part. He didn't think the first three payments would've appeared particularly concerning or suspicious to Revolut. But he thought Revolut should've been concerned by the point of the fourth payment. And as the payment was identifiably going to a crypto provider, which carries a known fraud risk, Revolut ought to have provided a tailored written scam warning – setting out the key features of crypto scams - to Miss W before processing

it. He thought this most likely would've resonated with Miss W and prevented her from making the payment.

Our Investigator thought Miss W should take some responsibility for her loss too. This was because, although Miss W says she did online checks on AT at the time, there were multiple negative reviews available that warned they were a scam firm. And given the family member was able to identify it was a scam from the research they undertook, it's reasonable to assume Miss W could've similarly done this. Our Investigator also noted that the guaranteed returns and high-pressure sales tactics Miss W has said were used ought to have led her to question the legitimacy of the firm. Because of this, he thought it would be fair for Revolut to refund 50% of the last two payments and pay 8% simple interest.

C confirmed Miss W's acceptance.

Revolut didn't agree with our Investigator. In short, they added:

- This is a 'self-to-self' scenario in which Miss W owned and controlled the beneficiary account to which the payments were sent. Hence, the fraudulent activity didn't occur on Miss W's Revolut account – as the payments were made to a legitimate crypto exchange before being sent to the scam platform.
- The transactions weren't out of character or unexpected with the typical way an electronic money institution (EMI) account is used – particularly as high street banks have started restricting their customers from sending money to crypto exchanges (which is an entirely legitimate activity). Typically, this type of account is opened and used to facilitate payments of a specific purpose and often not used as a main account.
- 'Self-to-self' payments don't meet the Dispute Resolution Rules ("DISP Rules"), nor the Contingent Reimbursement Model (CRM) code or incoming mandatory reimbursement rules definition of an Authorised Push Payment (APP) scam.
- It is entirely relevant to consider possible other bank interventions – as the funds originated from Miss W's own external bank account. As such, they believe it should be considered by the Financial Ombudsman in tandem with this complaint. At the very least, whether Miss W was warned by their external bank is relevant to whether she acted negligently in disregarding any such warnings.
- It might be appropriate for the Financial Ombudsman to exercise its powers under DISP to inform Miss W that it could be appropriate to make a complaint against another firm if necessary.
- It's irrational to hold Revolut responsible for any of the loss where it is only an intermediate link in a chain of transactions.

Our Investigator acknowledged Revolut's points but his view remained the same. In short, he explained:

- While Miss W may have paid money to another account held in her own name, rather than directly to the fraudsters, Revolut ought to have been aware of multi-stage scams involving crypto. And so, as a matter of good practice, been on the lookout for payments presenting an additional risk. In this case, he was satisfied that this risk was apparent by the fourth payment – and so, Revolut should've provided the tailored written scam warning or made further enquiries before processing it. Had this happened, he thought the scam would've been uncovered and Miss W's losses would've been prevented at that time.
- While the money originated from another FCA regulated firm, only this complaint has been brought to the Financial Ombudsman for us to consider. And the Financial Ombudsman cannot compel Miss W to bring a complaint about another firm.

- He contacted the bank in which the funds originated from and found that the only written warning provided to Miss W wasn't related to crypto scams (as the bank weren't able to establish the payments were being made for that purpose). Therefore, he didn't think the warning would've resonated with Miss W in the same way a tailored crypto warning from Revolut would have.

Revolut remained in disagreement with our Investigator and so, the matter 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 EMI such as Revolut is expected to process payments and withdrawals that a customer authorises them 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 Miss W 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 their 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 their 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 they suspected their 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 May/June 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;
- 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 May/June 2023, Revolut, whereby if they identified a scam risk associated with a card payment through their automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through their in-app chat).

I am also mindful that:

- Electronic Money Institutions like Revolut are required to conduct their business with "due skill, care and diligence" (FCA Principle for Businesses 2), "integrity" (FCA Principle for Businesses 1) and a firm "must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems" (FCA Principle for Businesses 3).
- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the *"Financial crime: a guide for firms".*
- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.

- The October 2017, BSI Code, 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 crypto when considering the scams that their 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 crypto 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 crypto 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 they 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 May/June 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 their 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 crypto 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 May/June 2023, Revolut should in any event have taken these steps.

Should Revolut have recognised that Miss W was at risk of financial harm from fraud?

It isn't in dispute that Miss W has fallen victim to a cruel scam here, nor that she authorised the payments she made by debit card to her crypto wallet (from where that crypto was

subsequently transferred to the scammer).

Whilst I have set out the circumstances which led Miss W to make the payments using her 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 them upon which to discern whether any of the payments presented an increased risk that Miss W might be the victim of a scam.

I'm aware that crypto exchanges, like the one Miss W made her payments to here, generally stipulate that the card used to purchase crypto at their 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, they could have reasonably assumed that the payments would be credited to a crypto wallet held in Miss W's name.

By May 2023, when these transactions took place, firms like Revolut had been aware of the risk of multi-stage scams involving crypto for some time. Scams involving crypto have increased over time. The FCA and Action Fraud published warnings about crypto scams in mid-2018 and figures published by the latter show that losses suffered to crypto scams have continued to increase since. They reached record levels in 2022. During that time, crypto 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 crypto using their bank accounts or increase friction in relation to crypto related payments, owing to the elevated risk associated with such transactions. And by May 2023, when the first of these payments took place, further restrictions were in place. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase crypto 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 crypto 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 crypto 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 crypto 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 Miss W made in May/June 2023, Revolut ought fairly and reasonably to have recognised that their customers could be at an increased risk of fraud when using their services to purchase crypto, notwithstanding that the payment would often be made to a crypto wallet in the consumer's own name.

To be clear, I'm not suggesting that, as a general principle, Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees. As I've set out in some detail above, it is the specific risk associated with crypto in May/June 2023 that, in some circumstances, should have caused Revolut to consider transactions to crypto 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 their 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 crypto, I don't think the fact payments in this case were going to an account held in Miss W'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, they ought to have identified that Miss W might be at a heightened risk of fraud that merited their intervention.

While Revolut should've identified the payments were going to a crypto provider (the merchant is a well-known crypto provider), the first three payments were low in value. And so, I don't think there would've been enough reason for Revolut to suspect that they might have been made in relation to scam.

The fourth payment however, which again would've been identifiable as going to a crypto provider, was significantly greater in value than those that preceeded it. And given the account opening reason provided by Miss W was 'overseas transfers', it would've been clear to Revolut that she wasn't using the acccount for this purpose by this point – so, this contradictory account usage should've been of concern to Revolut. I understand Revolut needs to take an appropriate line between protecting against fraud and not unduly hindering legitimate transactions. But given what Revolut knew about the destination of the payment, I think the circumstances should have led Revolut to consider that Miss W was at a 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 Miss W before this payment went ahead.

To be clear, I do not suggest that Revolut should provide a warning for every payment made to crypto. Instead, as I've explained, I think it was the combination of the value of the payment (which was significantly greater than those that preceded it), the fact it went to a crypto provider and that it was at odds with the account opening reason given By Miss W which ought to have prompted a warning.

What did Revolut do to warn Miss W?

I haven't seen anything to show Revolut provided a warning to Miss W before processing any of the payments.

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 Miss W made the 6 June 2023 payment, knowing (or strongly suspecting) that the payment was going to a crypto provider, to have provided a tailored warning that was specifically about the risk of crypto 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 crypto

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 crypto scams – crypto 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 Miss W 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 Miss W suffered from the fourth payment?

On balance, I think a specific warning covering off the key features of crypto investment scams would've prevented Miss W suffering her loss from this point. This is because there were several key hallmarks of common crypto investment scams present in the circumstances of Miss W's payments - such as finding the investment through an advertisement on social media that was endorsed by a public figure, being assisted by a broker, the use of remote access software and initial deposits that quickly increased in value (and which led to pressure to make deposits of a greater amount).

There's limited evidence of the communication between Miss W and the scammer. And so, I haven't seen anything to suggest that Miss W was asked, or agreed to, disregard any warning provided by Revolut. I've also seen no indication that Miss W expressed mistrust of Revolut or financial firms in general. And I understand that Miss W sought the opinion of a family member when AT applied pressure on her to pay more fees (due to an increase in profits). Because of this, I've no reason to think Miss W wouldn't have listened to the advice of Revolut.

At which point, I note that Miss W did receive a written warning from the bank the funds originated from. But this warning wasn't tailored to crypto investment scams – as the bank wasn't aware it was being used for this purpose, nor would they have been able to identify it was from the beneficiary (as it was going to Miss W's Revolut account, not the crypto exchange). Because of this, the warning presented to Miss W wasn't relevant to her circumstances and didn't cover off the key features of crypto investment scams that I've referred to above. It follows that I've not seen anything to show Miss W ignored warnings provided to her that were relevant to the scam she fell victim to, and which she ought reasonably to have heeded.

Therefore, on the balance of probabilities, had Revolut provided Miss W with an impactful warning that gave details about crypto investment scams and how she could protect herself from the risk of fraud, I believe it would have resonated with her. Miss W could have paused and looked more closely into AT before proceeding, as well as making further enquiries into crypto scams (as she later did with the assistance of a family member). I'm satisfied that a timely warning to Miss W from Revolut would very likely have caused her to take the steps she did later take – thereby revealing the scam and preventing her losses of $5,173 and £3,000.

Is it fair and reasonable for Revolut to be held responsible for Miss W's loss?

In reaching my decision, I have taken into account that this payment was made to another financial business (a crypto exchange) and that it was funded from another account at a regulated financial business held in Miss W's name and control.

But as I've set out in some detail above, I think that Revolut still should have recognised that Miss W might have been at risk of financial harm from fraud when she made the 6 June 2023 payment, and in those circumstances, they should have declined the payment and made further enquiries. If they had taken those steps, I am satisfied they would have prevented the loss Miss W suffered. The fact that the money used to fund the scam came from elsewhere and wasn't lost at the point it was transferred to Miss W's own account does not alter that fact and I think Revolut can fairly be held responsible for Miss W'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 Miss W 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 Miss W could instead, or in addition, have sought to complain against those firms. But Miss W 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 a consumer'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 Miss W's loss from the $5,173 payment made on 6 June 2023 onwards (subject to a deduction for Miss W's own contribution which I will consider below). As I have explained, the potential for multi-stage scams, particularly those involving crypto, ought to have been well known to Revolut. And as a matter of good practice and as a step to comply with its regulatory requirements, I consider Revolut should have been on the look-out for payments presenting an additional scam risk including those involving multi-stage scams.

Furthermore, I'm aware that Revolut has referenced the CRM code and the PSR's reimbursement scheme for APP scams. But Revolut is not a signatory of the CRM code, and these payments wouldn't have been covered by it anyway. Nor would the payments be covered by the PSR's reimbursement scheme – as it wasn't in force when these payments were made, it isn't retrospective, and it doesn't cover card payments. I've therefore not sought to apply either here. I've explained in some detail why I think it's fair and reasonable that Revolut ought to have identified that Miss W may have been at risk of financial harm from fraud and the steps they should have taken before allowing the final payment to leave her account.

Should Miss W bear any responsibility for her losses?

I've thought about whether Miss W should bear any responsibility for her loss. In doing so, I've considered what the law says about contributory negligence, as well as what I consider to be fair and reasonable in all of the circumstances of this complaint including taking into account Miss W's own actions and responsibility for the losses she has suffered.

When considering whether a consumer has contributed to their own loss, I must consider whether the consumer's actions showed a lack of care that goes beyond what we would expect from a reasonable person. I must also be satisfied that the lack of care directly contributed to the individual's losses.

Here, I consider that there were sophisticated aspects to this scam – not least the apparently credible and professional looking platform which showed Miss W her investment growth/profit. But there was the spoofed feature on a financial information website ran by a well-known public figure endorsing AT. And I also understand Miss W spoke with AT, at prearranged times, and she says they came across highly professional and knowledgeable about crypto too – thereby reassuring her about the legitimacy of the investment opportunity.

I have however considered that Miss W says she carried out online checks on AT online before investing but didn't find any negative reviews. Having carried out my own historical internet search however, I found a significant number of negative reviews on a well-known review website that appeared as a top search result. And I think this would've been easily accessible to Miss W at the time – and was likely what she and her family member found when carrying out further due diligence at the point the additional fees were requested by the scammer.

I therefore think Miss W ought reasonably to have found these negative reviews had she undertaken the due diligence she said she did. And the reviews were very clear in that many customers of AT considered them to a scam company – including references to a small initial deposit before significant pressure being applied to invest more, as well withdrawal and tax fees being payable. I think such reviews should've given reason for Miss W to question whether AT and the investment opportunity was legitimate. Thereby prompting her to take greater caution before proceeding – including, for example, seeking advice from her family friend (as she later did), a financial adviser or even her existing banking provider. If Miss W had done so, then I consider she would've most likely uncovered that she was being scammed – thereby preventing her losses.

I've concluded, on balance, that it would be fair to reduce the amount Revolut pays Miss W in relation to the last two payments because of her role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

Could Revolut have done anything to recover Miss W's money?

The payments were made by card to a legitimate crypto exchange. Miss W sent that crypto to the fraudsters. So, Revolut would not have been able to recover the funds. In addition, I don't consider that a chargeback would have had any prospect of success given there's no dispute that the crypto exchange provided crypto to Miss W, which she subsequently sent to the fraudsters.

Putting things right

I think it is fair that Revolut refund 50% of the last two payments Miss W made to the scam - $2,586.50 and £1,500. Revolut should use their exchange rate from 6 June 2023 to calculate the loss for the USD payment in pounds sterling. Revolut should also add 8% simple interest to the payments to compensate Miss W for her loss of the use of money that she might otherwise have used.

My final decision

My final decision is that I uphold this complaint in part. I direct Revolut Ltd to pay Miss W:

- 50% of the last two scam payments (as directed above);
- 8% simple interest, per year, from the date of each payment to the date of settlement less any tax lawfully deductible.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss W to accept or reject my decision before 25 February 2025.

Daniel O'Dell
Ombudsman