DRN-4604486

The complaint

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

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 Mrs F was researching investment options online and came across an investment firm, which I'll refer to as 'U', that we now know to be a scam. Mrs F reviewed U's website, which appeared genuine to her, and completed an online form whereby she provided her contact details. U then called Mrs F and explained how she could invest with them.

Under the belief U were legitimate, Mrs F decided to invest – with U's trading platform showing her investment growth/profit. As part of the investment scam, Mrs F made the following payments to U's trading platform via a legitimate crypto exchange:

Transaction date	Type of transaction	Amount
24 May 2023	Debit card	£255
24 May 2023	Debit card	£490
31 May 2023	Debit card	£500
29 June 2023	Debit card	£3,000
	Total loss:	£4,245

Mrs F has explained that U continued to pressure her into investing more funds. And that this intense pressure raised her suspicions and so, she contacted a friend about it. Mrs F, with the assistance of her friend, searched U online and uncovered they weren't legitimate.

Mrs F reported the scam payments to Revolut on 2 July 2023. And she confirmed that, as part of the scam, she'd installed remote desktop software – which Revolut directed her to remove. Revolut also explained how Mrs F could submit a chargeback claim, which she did for the first transaction. But as she was having difficulties raising chargebacks for the rest, Revolut raised those for Mrs F.

On 14 July 2023 Revolut told Mrs F they couldn't dispute the scam payments as she'd authorised them through 3D Secure (3DS). Mrs F then raised a complaint with Revolut on 3 October 2023 as she was unhappy they wouldn't refund her. She said that, despite providing Revolut with all the necessary evidence and details of the fraudulent activity, they refused to take responsibility and offered her no support. She believed Revolut failed in their duty to protect her from fraud and requested reimbursement of her loss to the scam.

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

- Their agents, in chat, followed their processes correctly – disputing the fraudulent transactions via the chargeback process.
- The chargeback process is framed by a very detailed and consistent set of rules. And, essentially, 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 Mrs F'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.

Mrs F referred her complaint to the Financial Ombudsman. Our Investigator thought it should be upheld in part. She didn't think the first three payments would've appeared particularly concerning or suspicious to Revolut. But as the third payment of £3,000 was significantly higher in value and identifiable as going to a crypto merchant, Revolut should've provided a tailored written scam warning to Mrs F before processing it. This warning should've set out the key features of crypto scams, such as the risks of an adviser/broker being involved and moving funds to an investment platform to be managed by that person. Had this happened, she thought Mrs F would likely have responded positively to it – realising the similarities to her situation – and not gone ahead with the payment.

Our Investigator thought Mrs F should take some responsibility for her loss too. This was because Mrs F didn't carry out any research or due diligence on U before investing, but instead, she relied on speaking with the scammer. Had she searched U online, she would've come across a website that had a negative review posted about U prior to her first scam payment. So, our Investigator thought it would be fair for Revolut to refund 50% of the final payment (£1,500) and pay 8% simple interest.

Revolut didn't agree with out Investigator and asked for the matter to be referred to an Ombudsman. In short, Revolut added:

- Mrs F acted with gross negligence; they explained:
    - Under the Payment Services Regulator's (PSR) reimbursement scheme for Authorised Push Payments (APP) scams (which was only proposed at the time of their submission) and the Contingent Reimbursement Model (CRM) code, payment service providers are exempted if the customer has acted with gross negligence.
    - Mrs F installed remote desktop software, which can induce security breaches due to the arbitrary access to sensitive information one can obtain
    - Negative reviews regarding this investment opportunity were already available online, and it was Mrs F's duty to further scrutinise the investment before committing to it financially. This demonstrates the requisite degree of carelessness required to displace any liability Revolut might otherwise have had.
    - The Ombudsman upholding a complaint, in that Revolut should reimburse the customer, without proper regard to the customer's lack of care is irrational.
- Revolut is bound by contract, applicable regulations and common law to execute Mrs F's valid payment instructions. And they do not consider any of the limited exceptions to Revolut's duty apply in this case.
- In accordance with the 'personal terms', Revolut agreed to execute transfers in accordance with the instructions Mrs F made by using her card.

- The Payment Services Regulations 2017 also apply in this case – with these imposing obligations on payment service providers to promptly execute authorised payment transactions. Revolut recognises their obligations to put in adequate procedures to counter the risk that it may be used to further financial crime (and has such systems and controls in place), but that duty does not go as far as to require Revolut to decline a payment.
- The duty to execute valid payment instructions doesn't require Revolut to assess the commercial wisdom or potential financial loss of a proposed transaction. This point was recognised in the Supreme Court's judgment in Philipp vs Barclays Bank UK PLC.
- Revolut has adequate systems and controls in place to detect unusual or suspicious transactions. However, is it relevant to highlight the payments went to a legitimate merchant; the card payments in question were successfully authorised with the 3DS; it is clear Mrs F's primary intention when using her account was to receive payments from her external account and perform card payments; the payments were made to a crypto account in Mrs F's name and control; and the type of account which Mrs F has used is not a current account and Revolut are not a bank but an Electronic Money Institution (EMI). Therefore, they're not persuaded such payments ought to have raised suspicions.
- There was no uncertainty as to the validity of Mrs F's instruction(s), and any delay by Revolut to execute an instruction would've amounted to a breach of their duty to Mrs F.

I sent my provisional decision on this complaint on 7 November 2024. I said:

> *"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 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 F 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 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 it identified a scam risk associated with a card payment through its automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat).

I am also mindful that:

- *Electronic Money Institutions like Revolut are required to conduct their business with "due skill, care and diligence" (FCA Principle for Businesses 2), "integrity" (FCA Principle for Businesses 1) and a firm "must take reasonable care to organise and control its affairs responsibly and effectively, with*

adequate risk management systems" (FCA Principle for Businesses 3).

- *Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the "Financial crime: a guide for firms".*
- *Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.*
- *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 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 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 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 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 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 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 Mrs F was at risk of financial harm from fraud?

It isn't in dispute that Mrs F 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 Mrs F 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 it upon which to discern whether any of the payments presented an increased risk that Mrs F might be the victim of a scam.

I'm aware that crypto exchanges, like the one Mrs F made her payments to here, generally stipulate that the card used to purchase crypto 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 payments would be credited to a crypto wallet held in Mrs F'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 Mrs F made in May/June 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 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 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 crypto, I don't think the fact payments in this case were going to an account held in Mrs F'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 F might be at a heightened risk of fraud that merited its 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 proceeded it. 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 Mrs F 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 Mrs F 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 Mrs F's prior account

usage) and that the fact it went to a crypto provider which ought to have prompted a warning.

What did Revolut do to warn Mrs F?

Revolut has confirmed that it didn't provide scam warnings to Mrs F before processing any of the payments. But rather, the only warning provided was part of the 3DS authentication process.

I don't think this was sufficient or proportionate to the risk the £3,000 payment presented (as it wasn't specific to crypto scams). I think Revolut needed to do more.

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 Mrs F attempted to make the 29 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 crypto investment scams, for example referring to: an 'account manager', 'broker' or 'trader' acting on their behalf; moving crypto to a third-party trading platform; 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 F 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 Mrs F suffered from the fourth payment?

On balance, I think a specific warning covering off the key features of crypto investment scams would've prevented Mrs F suffering her loss (£3,000). This is because there were several key hallmarks of common crypto investment scams present in the circumstances of Mr F's payment(s). This includes Mrs F being assisted by a third-party broker who was directing her to move funds to their trading platform, being asked to download remote access software, and making smaller deposits that increased quickly in value before being pressured into making deposits of a significantly greater amount.

From the chat conversations between Mrs F and the scammer that I've seen, I haven't seen anything to show that Mrs F was asked, or agreed to, disregard any

warning provided byRevolut. I've also seen no indication that Mrs F expressed mistrust of Revolut or financial firms in general. Neither do I think that the conversation demonstrates a closeness of relationship that Revolut would have found difficult to counter through a warning. And I understand that Mrs F sought the opinion of her friend when U applied pressure on her to invest more funds. Because of this, I'm not persuaded Mrs F was so taken in by the scammers that she wouldn't have listened to the advice of Revolut. And I note that I've also seen no evidence that Mrs F was provided with warnings by the firm from which the funds used for the scam appear to have originated.

Therefore, on the balance of probabilities, had Revolut provided Mrs F 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. Mrs F could have paused and looked more closely into U before proceeding, as well as making further enquiries into crypto scams (as she later did, of her own accord with the assistance of a friend, following this payment). I'm satisfied that a timely warning to Mrs F from Revolut would very likely have caused her to take the steps she did take later – thereby revealing the scam and preventing her £3,000 loss.

Is it fair and reasonable for Revolut to be held responsible for Mrs F'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 Mrs F's name and control.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mrs F might have been at risk of financial harm from fraud when she made the 29 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 Mrs F 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 Mrs F's own account does not alter that fact and I think Revolut can fairly be held responsible for Mrs F'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 F 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 F could instead, or in addition, have sought to complain against those firms. But Mrs F 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 Mrs F's loss

from the £3,000 payment made on 29 June 2023 (subject to a deduction for Mrs F'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 – and their exemptions if the customer has acted with gross negligence. 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 Mrs F 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 Mrs F bear any responsibility for her losses?

I've thought about whether Mrs F 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 Mrs F'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 Mrs F her investment growth/profit. I'm also mindful that Mrs F spoke with U on several occasions, and that 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 Mrs F has confirmed that she didn't carry out any due diligence on U before investing with them. Instead, she relied on her conversations with U and, from this and their website, she felt reassured they were genuine. As an inexperienced investor, I think it was understandable that Mrs F wouldn't have necessarily known the types of checks she could carry out to verify the legitimacy of an investment firm – without, say, the direction of Revolut. But I'm aware that Revolut, and our Investigator, referred to there being a negative review(s) about U available online prior to Mrs F making her first scam payment.

It's not unreasonable, given Mrs F came across U from researching investment options online, to have expected her to have carried out some checks on U beyond relying on their own website – which isn't the most reliable method of verification. But having carried out my own historical internet search of U, there appears to be very little information about U available prior to 24 May 2023. And the negative review that our Investigator referred to wasn't a prominent search result. Because of this, I'm not confident that Mrs F would've necessarily found this negative review from an internet

search of U at the time.

But even if Mrs F did find it, I'm not persuaded that one negative review alone would've been enough for her to have realised U was a scam firm – particularly as, in the review, the reviewer confirms they didn't actually register with U or use their services. Furthermore, I've also found that there were two positive reviews about U available on another website – which I consider to be a well-respected and established review website - that preceded Mrs F's first scam payment. I think, given this site's greater online presence for business reviews, it's more likely that Mrs F would've found and relied on these positive reviews had she carried out such checks before investing with U.

It follows that, having considered the overall circumstances of what happened, I think Mrs F could've done more to protect herself before proceeding to invest with U. But even if she had, I'm not persuaded this would've made a difference – as I think she would've likely been reassured by the positive reviews about U that were available at the time and gone ahead with the payments. It follows that I don't think Mrs F's actions (or in action) directly contributed to her losses.

So, while Mrs F may have put misplaced trust in U, likely because of the regular conversations and their professional manner, I don't think it would be fair and reasonable to reduce the award based on contributary negligence in the circumstances of this complaint.

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

The payments were made by card to a legitimate crypto exchange. Mrs F 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 Mrs F, which she subsequently sent to the fraudsters.

Putting things right

I think it is fair that Revolut refund Mrs F the final payment she made to the scam. They should also add 8% simple interest to the payment to compensate Mrs F for her loss of the use of money that she might otherwise have used.

My provisional decision

My provisional decision is that I uphold this complaint in part. I intend to direct Revolut Ltd to pay Mrs F

- *The final scam payment - £3,000.*
- *8% simple interest, per year, on £3,000 calculated from 29 June 2023 to the date of settlement less any tax lawfully deductible."*

Mrs F accepted my provisional decision. But Revolut didn't respond to it.

Now that both parties have had an opportunity to respond, I can proceed to making my final decision on Mrs F's complaint.

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 the absence of any further points for my consideration, I see no reason to depart from the above. I therefore remain of the view that Revolut is responsible for the loss Mrs F suffered in relation to the final payment of £3,000. And that it wouldn't be reasonable to reduce the award due to contributory negligence on Mrs F's part in these circumstances. It follows that I think Revolut should refund £3,000 to Mrs F and pay 8% simple interest to recognise the loss of use of money she suffered.

My final decision

I uphold this complaint. I direct Revolut Ltd to pay Mrs F:

- The final scam payment - £3,000.
- 8% simple interest, per year, on £3,000 calculated from 29 June 2023 to the date of settlement less any tax lawfully deductible.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs F to accept or reject my decision before 20 December 2024.

Daniel O'Dell
Ombudsman