DRN-5222424

The complaint

Miss A complains Revolut Ltd won't refund payments she lost when she was the victim of a cryptocurrency investment scam.

Miss A is professionally represented, however, to keep things simple, I'll refer to Miss A throughout my decision.

What happened

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

Miss A was sent an online newspaper article from her mother about a cryptocurrency investment opportunity with a firm I'll refer to as 'O', which we now know to be a scam firm. Miss A followed the link and went through to O's website, whereby she was impressed with how professional and genuine the opportunity looked. Miss A also carried out background research on O online, as well as asking a close friend to do the same, but they both didn't find anything to indicate it was a scam.

In November 2022, Miss A completed O's online sign-up form that required photo identification and her passport - which further convinced her the opportunity was genuine. Shortly after, an advisor from O, who would also be trading on her behalf, contacted Miss A and asked her for an initial investment of £250 to set up the account. She was also asked to open an account with Revolut where future investments would be withdrawn from and the profits paid into.

After seeing her initial investment fluctuating in profits, exactly as the advisor had told her it would, O told Miss A she would need to invest greater amounts. And during the course of the scam, O convinced Miss A to take out multiple loans to increase her investment, as her balance had gone into negative. She was told by O this was required to prevent her from owing a large amount of money, if her profits continued to drop, so she duly proceeded to take out the loans.

Miss A received the loans into her other banking provider, which I'll refer to as 'N'. She then transferred the funds from N to her Revolut account, before forwarding it on to O. Miss A made the following payments to O's trading platform via legitimate cryptocurrency exchanges in her own name:

Payment	Date	Payment Method	To	Amount
1	30/11/2022	Card payment	Cryptocurrency provider 1	£1,950
2	02/12/2022	Card payment	Cryptocurrency provider 2	£5,000
3	06/12/2022	Card payment	Cryptocurrency	£5,000

			provider 2	
4	12/12/2022	Card payment	Cryptocurrency provider 3	£4,634.55
5	09/01/2023	Card payment	Cryptocurrency provider 2	£5,252.49
			Total loss:	£21,837.04

Miss A saw her funds fluctuate on O's trading platform as the advisor continued to trade on her behalf. The advisor tried to convince her to increase her investment by borrowing money from her family. Miss A felt the current investment was sufficient and didn't feel that more investment was necessary. When she attempted to make a withdrawal, Miss A was told she would need to purchase 25% of her account worth in Bitcoin. She mentioned she didn't have the funds to do this and wouldn't be getting any further loans or borrowing. She then received continuous calls from a third-party firm informing her that her account with O had been flagged up as suspicious. At this point, she carried out some further due diligence on the company that contacted her, which made her question the legitimacy of O. When she questioned the advisor at O about the information she had found, the advisor became hostile in their response. Miss A then involved her sibling and realised she had been a victim of a scam.

Miss A raised a complaint with Revolut. In short, she said:

- The payments were made as part of a cruel investment scam.
- Revolut allowed £21,837.04 to pass through a newly opened Revolut account without any proper checks or effectively intervening in order to investigate the very obvious fraud taking place.
- The newly opened Revolut account immediately received high value credits that were transferred out in line with several patterns of fraud and financial crime, which Revolut failed to pick up on.
- No scam warnings or messages about investment scams were provided at the time the payments were being made.
- The payments were unusual and had Revolut stepped in and asked more probing questions about the nature of the payments, she would not have proceeded with the transactions.
- She was vulnerable before and during the scam as she was suffering from anxiety and depression which made her more susceptible to being scammed.
- To settle the complaint, she wanted Revolut to provide her a refund, pay 8% simple interest and £300 in compensation.

Revolut didn't uphold the complaint. In short, the final response letter said:

- As the transactions in question were related to card payments, the method used to challenge these transactions is known as "chargeback". 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.
- Revolut's chargeback team needs to verify if the conditions for fraud chargeback claims are met which will result in a thorough examination being carried out and the findings communicated to Miss A.

Revolut then subsequently informed Miss A of the outcome of the claim, which was that they had no right to dispute them as they'd found no traces of fraudulent activity on Miss A'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. Revolut also added, 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.

As a result, the complaint was raised to the Financial Ombudsman. Our Investigator thought the complaint should be upheld in part and asked Revolut to provide a full refund of the final payment, plus 8% simple interest.

Miss A confirmed her acceptance.

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

- This is a 'self-to-self' scenario in which Miss A owned and controlled the beneficiary accounts to which the payments were sent. Hence, the fraudulent activity didn't occur on Miss A's Revolut account – as the payments being made were to perform legitimate cryptocurrency purchases to accounts held in Miss A's own name.
- The type of payments made were not out of character nor unexpected payments with the typical way in which an Electronic Money Institute (EMI) account is used.
- The recent reliance by the Financial Ombudsman on R (on the application of Portal Financial Services LLP) v FOS [2022] EWHC 710 (Admin) is misconceived and amounts to a legal error.
-
- It is entirely relevant to consider possible other bank interventions – as the funds that originated with Revolut came from Miss A's own external bank account.
- While they recognise the Financial Ombudsman may have considerable sympathy for customers who have been defrauded, this allocation of responsibility is at odds with the approach the statutory regulator (i.e the PSR) deems appropriate and is irrational.
- It is irrational (and illogical) to hold Revolut liable for customer losses in circumstances where Revolut is merely an intermediate link, and there are typically other financial institutions in the payment chain that have comparatively greater data on the customer than Revolut, but which the Financial Ombudsman hasn't held responsible in the same way as Revolut.

As no agreement could be reached, Miss A's complaint has been passed to me to decide.

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 deciding what's fair and reasonable, I am required to take into account relevant law and regulations, regulators' rules, guidance and standards, and codes of practise; and where appropriate, I must also take into account what I consider to have been good industry practise at the time.

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 Miss A 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 November 2022 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 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.

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

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

- 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 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 practise (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 November 2022 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 November 2022, Revolut should in any event have taken these steps.

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

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

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

Whilst I have set out the circumstances which led Miss A 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 the time, Revolut had no genuine account activity to compare the scam-related activity against, as Miss A opened a Revolut account for the purpose of this scam.

On balance, considering the value of the first payment Miss A made, taking into account that Revolut needs to take an appropriate line between protecting against fraud and not unduly hindering legitimate transactions, I don't think Revolut ought to have been sufficiently concerned about this payment. Also, this was a one-off payment to a cryptocurrency exchange provider for a relatively modest value.
By January 2023, when Miss A made payment 5, 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. And by January 2023, when Miss A made payment 5, 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 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 payment 5 Miss A 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. And as I've set out 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 payment 5 was going to an account held in Miss A's own name should have led Revolut to believe there wasn't a risk of fraud.

What did Revolut do to warn Miss A?

I haven't seen anything to show Revolut provided a warning to Miss A 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 payment 5 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 A attempted to make the final payment, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. 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.

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, and I recognise that a warning of that kind could not have covered off all scenarios, however, I think it would have been a proportionate way for Revolut to minimise the risk of financial harm to Miss A 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 loss Miss A suffered for the last payment?

I've thought carefully about whether such a warning would've resonated with Miss A for the final payment of £5,252.49, and to the extent whereby she wouldn't have proceeded with making it. Having done so, I think it would.

There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of the final payment made by Miss A. This includes finding the investment opportunity through an advertisement, being assisted by a broker, being asked to make a small initial deposit.

I've also read the instant message conversations between Miss A and the fraudsters. The conversation shows that shortly after the final payment was made, Miss A kept asking O about a withdrawal she'd requested and when this would be approved. The following day Miss A had also questioned the fraudster if information she'd been sent by O was *'real or fraud'*. While this happened after the final payment was made, I think it indicates that it wouldn't have taken much persuasion (that a warning could have provided) to convince Miss A that there could be a risk she was falling victim to a scam.
From the chat conversation, I think Miss A was clearly worried about her financial position and showed signs of desperation in trying to recover what she had already paid towards the scam. Because of this, I think a warning – of the type described – would've very likely given Miss A enough reason to question the legitimacy of O. In turn, Miss A would've like sought reassurance from the family member (as she later did).

Revolut have questioned whether any other financial business involved in the scam provided warnings that Miss A should have taken notice of. Here, N has confirmed that the only warning they provided was when Ms A set up her Revolut account as new payee. Unfortunately, they cannot confirm what warning was shown, as it was dependent on the payment purpose selected, but it was most likely *"moving money to one of my other accounts"*. This however, while an accurate description of why Ms A was making that payment(s) from her N account, didn't provide Ms A with the relevant information for cryptocurrency investment scams. So, I don't think Ms A ignored a warning relevant to her situation.

I've also found nothing within the conversations between Miss A and the fraudsters to suggest she was asked, or agreed to, disregard any warning provided by Revolut. And I've seen no indication that Miss A expressed mistrust of Revolut or financial firms in general. The evidence I've seen persuades me that Miss A was not so taken in by the fraudsters that she wouldn't have listened to the advice of Revolut.

Therefore, on the balance of probabilities, had Revolut provided Miss A with an impactful warning on the final payment that gave details about cryptocurrency investment scams and how she could protect herself from the risk of fraud, I believe it would have resonated with her. I'm satisfied that a timely warning to Miss A from Revolut would very likely have revealed the scam and prevented her further losses.

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

In reaching my decision about what is fair and reasonable, I have taken into account that Miss A purchased cryptocurrency which credited e-wallets held in her own name, rather than making a payment directly to the fraudsters. 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 fraudsters.

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

Revolut has also addressed an Administrative Court judgment, which was referred to in a decision on a separate complaint. As I have not referred to or relied on that judgment in reaching my conclusion in relation to the losses for which I consider it fair and reasonable to hold Revolut responsible, I do not intend to comment on it. I note that Revolut says that it has not asked me to analyse how damages would be apportioned in a hypothetical civil action but, rather, it is asking me to consider all of the facts of the case before me when considering what is fair and reasonable, including the role of all the other financial institutions involved.

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 payment 5 of Miss A's loss. 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 multistage scams

Should Miss A bear any responsibility for her losses?

I've thought about whether Miss A 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 A's own actions and if she 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. Having done so, I don't think that would be fair here.

Miss A was presented with the investment opportunity through what she had believed to be a genuine recommendation from her mother. So, there was nothing obviously suspicious about the way she came across the investment.

Miss A also hadn't invested in cryptocurrency before and so this was an area with which she was unfamiliar. This unfamiliarity was compounded by the sophisticated nature of the scam and the fact she believed the trading platform was genuine.

She's also explained she did some basic research as well as asking a friend to do similar, and they both didn't find anything negative about O. As an inexperienced investor, I think it was understandable that Miss A 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. So, I consider checking a well-known review website and seeking support from a friend was reasonable in the circumstances.

At which point, I'm aware that Revolut has said they couldn't find any positive reviews on this website. This is despite Miss A saying there was one single positive review listed at the time.

Having reviewed this website, Revolut correctly point out that there are only negative '1-star' reviews posted at this time – albeit these are dated subsequent to the payments Miss A. However, it is known that reviews can be removed. And on the reviews says, "*I think the positive reviews on this page are fake"*. This supports Miss A's claim that there was a positive review, and I don't think it was unreasonable for her to rely on it when deciding to proceed with the investment opportunity. And during the course of the scam, considering her investment inexperience, it is understandable why she relied heavily upon the guidance of O, whom she considered a legitimate investment firm.

So, taking all this into consideration, while Miss A may have been overly trusting of O, I don't think her actions were negligent to the point whereby it would be fair to reduce the award. But instead, I think Revolut's failure to undertake an appropriate intervention at payment five caused Miss A's loss.

Could Revolut have done anything to recover Miss A's funds?

The payments were made by card to two legitimate crypto exchange providers. Miss A 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 providers provided crypto to Miss A, which she subsequently sent to the fraudsters.

Compensation

The main cause for the upset was the scammer who persuaded Miss A to part with her funds. I haven't found any errors or delays to Revolut's investigation, so I don't think it would be fair and reasonable to award compensation in these circumstances.

Putting things right

I think it is fair that Revolut refund the last payment Miss A made to the scam.
I've also taken into consideration that Miss A took out multiple loans across various dates to funds the scam payments, which she has confirmed have now all been paid back. And as I'm satisfied Miss A was still deprived of the use of the funds that she might have otherwise used, to recognise this, I consider Revolut should pay 8% simple interest to the payment.

My final decision

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

- £5,252.49
- 8% simple interest, per year, from the date of the 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 A to accept or reject my decision before 8 July 2025.

Israr Ahmed
Ombudsman