

## The complaint

Mrs S complains that Revolut Ltd ('Revolut') hasn't protected her from losing money to an authorised push payment ('APP') investment scam.

In bringing her complaint, Mrs S has used the services of a professional representative. For ease of reading within this decision, I will refer to Mrs S throughout.

## What happened

The background to this complaint is well known to both parties, so I won't repeat everything in detail here. But in summary, I understand it to be as follows.

In August 2023 Mrs S came across an advert on a well-known social media platform for a company, whom I'll call 'J', that was advertising trading in cryptocurrency and other commodities such as gold and silver. Mrs S had seen the advert a number of times and as she was interested in what it was offering, filled out an enquiry form leaving her contact details. Mrs S was then contacted through a well-known messaging app by a representative of J. I'll call this person 'V'.

Mrs S says V sounded professional and knowledgeable and he quickly built up a rapport with her as he communicated with her in her native language. Mrs S says she checked J's website, and it looked well put together and professional and had positive reviews. Mrs S had to download J's trading platform and was given login details to access her account. Mrs S made an initial investment of £200 from an account held at one of her other banking providers. Mrs S says she saw good profits and V encouraged her to invest more. Mrs S on the instruction of V opened an account with Revolut and also an account with a cryptocurrency exchange provider – 'B'.

Sadly, Mrs S wasn't dealing with a legitimate company and was in fact dealing with fraudsters.

Mrs S proceeded to invest more and, as part of the scam, she made the following payments totalling €27,830.00, from her Revolut account.

No	Date	Time	Amount	To
1	15/08/2023	09:55	€5,000.00	Cryptocurrency account in Mrs S's name
2	16/08/2023	08:34	€10,800.00	Cryptocurrency account in Mrs S's name
3	17/08/2023	08:47	€5,400.00	Cryptocurrency account in Mrs S's name
4	21/08/2023	11:53	€6,630.00	Cryptocurrency account in Mrs S's name

Mrs S funded her Revolut account with transfers in from another bank account she held at another firm. The payments she then made from her Revolut account were to an account in her name with B, with Mrs S then exchanging the funds into cryptocurrency and sending them on to accounts controlled by the fraudsters.

Mrs S realised she'd been scammed when she attempted to withdraw funds from the investment. Mrs S also received communication / a letter on 22 August 2023 advising she needed to pay approximately €7,500 to cover an exchange rate difference to obtain a withdrawal of \$76,927.

Mrs S raised the matter with Revolut, but it didn't agree to reimburse Mrs S her loss.

Unhappy with Revolut's response Mrs S brought her complaint to this service. One of our Investigator's looked into things and thought the complaint should be upheld.

In summary, it was our Investigator's view that Revolut should have recognised that Mrs S could have been at a heightened risk of financial harm when she made Payment 2 (for €10,800) and that it should have intervened. It was our Investigator's view that appropriate intervention ought to have taken the form of human / staff intervention and had this intervention taken place the scam could have been prevented, and Mrs S wouldn't have lost her money from this point. Our Investigator also thought Mrs S shouldn't bear any responsibility for the loss.

Overall, our Investigator thought Revolut should refund Mrs S in full for Payments 2, 3 and 4 and that it should pay 8% simple interest on this amount from the date of the loss.

Through her representatives, Mrs S responded and agreed with our Investigator's opinion.

Revolut responded disagreeing. In summary, within its submissions to this service and in response to the view, it advised:

- Mrs S authorised the payments in question. And in accordance with the Payment Services Regulations 2017 ("PSR 2017"), and the general banking terms and conditions, Revolut should process authorised payments promptly. And as a starting point, Mrs S is liable for payments she has authorised.
- Proportionate and appropriate APP scam warnings were displayed to Mrs S when she made Payments 1 and 2. But Mrs S proceeded with each transaction despite its warnings and she wasn't truthful with some of her answers to the questions it asked her.
- It does not believe further intervention would have changed the outcome, as it considers it is plausible to assume that Mrs S would have persisted in her course of action regardless of any additional warning issued by Revolut.
- Mrs S opened the account solely for the purpose of the payments made as part of the scam. So Revolut had no previous transaction history and no basis of comparison to identify the payments as unusual or outside of Mrs S's normal behaviour.
- The type of account which Mrs S used is not a current account and Revolut are not a bank but an 'Electronic Money Institute' ('EMI') and typically this type of account is opened and used to facilitate payments such as the ones performed by Mrs S, so the type of payments being made were not out of character with the typical way in which an EMI account is used.
- Revolut does not owe a duty to prevent fraud or scams. It has no legal duty to prevent fraud and it must comply strictly and promptly with valid payment instructions. It does not need to concern itself with the wisdom of those instructions. And this was confirmed in the recent Supreme Court judgement in the case of Philipp v Barclays Bank UK plc [2023] UKSC 25.

- Revolut is bound by contract, applicable regulations, and the common law to execute valid payment instructions. The duty is strict and is subject to only very limited exceptions (for example if the customer has asked Revolut to act unlawfully).
- FOS have overstated Revolut's duty to its customers, and errors in law, by stating that Revolut should have "taken additional steps, or made additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud".
- Revolut served as an intermediary in the fraudulent transfers with Mrs S topping up her Revolut account with funds from her another banking provider and then transferring those funds on a cryptocurrency account in her name. The payments in question are in reality self-to-self payments. The fraudulent activity did not occur on the customer's Revolut account, as the payments being made were to perform legitimate cryptocurrency purchases to accounts held in the customer's own name.

As agreement couldn't be reached, the complaint has been passed to me for a final decision.

Having considered the complaint, I issued a provisional decision on 2 May 2025, as I intended on reaching a different conclusion to that of our Investigator. In short, I agreed with our Investigators findings that Revolut could have done more to prevent Mrs S's losses on Payments 2, 3 and 4, but I also considered Mrs S should bear some responsibility for her loss also. So, I considered Revolut should refund Mrs S 50% of Payments 2, 3 and 4 and pay 8% simple interest from the date of loss until date of settlement.

I gave both parties until 16 May 2025 in which to respond to my provisional decision and provide any more comments and evidence they wished for me to consider. Mrs S responded agreeing to the findings and outcome I had reached. Revolut didn't respond within the deadline set.

### **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.

As Mrs S has responded agreeing to my provisional decision and Revolut didn't respond, and as neither party has therefore given me anything else to consider, I see no reason to depart from my provisional findings. I'll confirm those findings below:

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 practice; and, where appropriate, I must also take into account what I consider to have been good industry practice at the time.

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 S modified the starting position described in *Philipp*, by 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"*.

So Revolut was required by the implied terms of its contract with Mrs S and the Payment Services Regulations to carry out their instructions promptly, except in the circumstances set out in its contract, which included where regulatory requirements meant it needed to carry out further checks.

Whether or not Revolut was required to refuse or delay a payment for one of the reasons set out in its contract, the basic implied requirement to carry out an instruction promptly did not in any event mean Revolut was required to carry out the payments immediately<sup>1</sup>. Revolut could comply with the requirement to carry out payments promptly while still giving fraud warnings, or making further enquiries, prior to making the payment.

And, I am satisfied that, taking into account longstanding regulatory expectations and requirements and what I consider to have been good industry practice at the time, Revolut should in August 2023 fairly and reasonably 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 (irrespective of whether it was also required by the express terms of its contract to do so).

---

<sup>1</sup> The Payment Services Regulation 2017 Reg. 86 states that "the payer's payment service provider must ensure that the amount of the payment transaction is credited to the payee's payment service provider's account **by the end of the business day following the time of receipt of the payment order**" (emphasis added).

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 do in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;<sup>2</sup>
- 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.

In reaching my conclusions about what Revolut ought fairly and reasonably to have done, I am also mindful that:

- EMIs 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<sup>3</sup>, 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).

---

<sup>2</sup> 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/](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/)

<sup>3</sup> BSI: PAS 17271: 2017” Protecting customers from financial harm as result of fraud or financial abuse”

- Since 31 July 2023, under the FCA's Consumer Duty<sup>4</sup>, regulated firms (like Revolut) must act to deliver good outcomes for customers (Principle 12) and must avoid causing foreseeable harm to retail customers (PRIN 2A.2.8R). Avoiding foreseeable harm includes ensuring all aspects of the design, terms, marketing, sale of and support for its products avoid causing foreseeable harm (PRIN 2A.2.10G). One example of foreseeable harm given by the FCA in its final non-handbook guidance on the application of the duty was *"consumers becoming victims to scams relating to their financial products for example, due to a firm's inadequate systems to detect/prevent scams or inadequate processes to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers"*<sup>5</sup>.
- 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.

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 August 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;
- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;
- 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.

---

<sup>4</sup> Prior to the Consumer Duty, FCA regulated firms were required to "pay due regard to the interests of its customers and treat them fairly." (FCA Principle for Businesses 6). As from 31 July 2023 the Consumer Duty applies to all open products and services.

<sup>5</sup> The Consumer Duty Finalised Guidance FG 22/5 (Paragraph 5.23)

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

It isn't in dispute that Mrs S has fallen victim to a cruel scam here, nor that she authorised the payments to the cryptocurrency account in her own name (from where she exchanged the fiat currency into cryptocurrency and subsequently transferred this to the scammer).

By August 2023, when these transactions took place, firms like Revolut had been aware of the risk of multi-stage scams involving cryptocurrency for some time. Scams involving cryptocurrency have increased over time. The FCA and Action Fraud published warnings about cryptocurrency scams in mid-2018 and figures published by the latter show that losses suffered to cryptocurrency scams have continued to increase since. They reached record levels in 2022. During that time, cryptocurrency was typically allowed to be purchased through many high street banks with few restrictions.

By the end of 2022, however, many of the high street banks had taken steps to either limit their customer's ability to purchase cryptocurrency using their bank accounts or increase friction in relation to cryptocurrency related payments, owing to the elevated risk associated with such transactions. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to purchase cryptocurrency with few restrictions. These restrictions – and the reasons for them – would have been well known across the industry.

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

So, taking into account all of the above I am satisfied that by the end of 2022, prior to the payments Mrs S made in August 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.

I'm also mindful of the fact that this was a new account. Mrs S only opened the account on the advice of the fraudster and the purpose of the account was for 'crypto'. That put Revolut in a more difficult position in respect of spotting payments that might have had an associated fraud risk because there was no historical data concerning any typical account usage that could've served as a basis of comparison. And the purpose Mrs S intended to use the account was for cryptocurrency.

That said, I agree with the Investigator's conclusions that it ought to have had concerns at the point Mrs S made the payment of €10,800.00 on 16 August 2023 (Payment 2). Mrs S had made a considerable payment to a cryptocurrency exchange provider – B, the day before. So, I find that the value of Payment 2 which was made the very next day alongside the fact that it was again being made to a third-party cryptocurrency exchange was significant enough to necessitate Revolut taking some steps to warn Mrs S as there was a very likely risk present that she could be at risk of falling victim to financial harm from fraud.

I have also considered that the account opening purpose was consistent with the transaction Mrs S was making. However, for reasons already explained, by the time this payment was made Revolut ought to have recognised that cryptocurrency transactions carried an elevated risk of the likelihood of the transaction being related to a fraud or scam. Therefore, I think it fair and reasonable to have expected Revolut to have had some concerns.

What did Revolut do to warn Mrs S?

From the evidence that has been shared with me, Revolut initially asked Mrs S a series of questions about Payment 1 and Payment 2. And then it didn't provide any further warnings or intervene for the remaining payments.

For Payment 1, Revolut asked Mrs S the following questions and received the following answers:

*"Please answer truthfully*

*If you're being scammed, the fraudster may ask you to hide the real reason for this payment*

**Answer:** I understand

**Question:** Is anyone telling you how to answer these questions?

*Is someone telling you which options to choose or telling you this is urgent?*

**Answer:** No, I am not being assisted through this questionnaire

**Question:** Why are you making this transfer?

*We'll only use this information to help protect your account*

**Answer:** As part of an investment

**Question:** What kind of investment?

*This helps us identify your level of risk*

**Answer:** Gains from cryptocurrency

**Question:** Have you been asked to install software?

*Scammers might ask you to install software (e.g. Anydesk) to view your screen, spy on your personal details and help you to set up your investment account*

**Answer:** No, I was not asked to install any software

**Question:** How did you discover this opportunity?

*Scammers use social media to entice victims by advertising fake investments. Well known celebrities or influencers may promote it to look legitimate*

**Answer:** Friend or family member

**Question:** Have you ever invested in crypto?

*Inexperienced investors are more likely to be scam targets*

**Answer:** Yes, I've invested in crypto before

**Question:** Have you researched the company?

**Answer:** Yes - I checked if the firm is on the FCA Register"

Having considered this carefully, I find Revolut's actions were appropriate to the potential risk identified in relation to Payment 1. I say this because Mrs S had opened the account with the sole purpose of making cryptocurrency transfers / payments. And here I think it is fair to say that Revolut, would have been satisfied from the answers it received that Mrs S was making a payment, that was likely going to her own account, and she had discovered the opportunity through friends and family, had invested in cryptocurrency before and ensured the firm she was dealing with was on the FCA register. So, I don't think Revolut needed to go further such as human intervention or direct Mrs S to its in-app chat to question her further about Payment 1.

I am also mindful that Mrs S says that the scammer was professional and had immediately built a rapport with her. By her own admission, Mrs S had confidence that the scammer was legitimate and that they were looking out for her best interests. As a result, she was persuaded to give the scammer remote access to her devices and willingly followed the scammer's instructions on how to open various accounts on different platforms. So, I'm not persuaded a tailored written warning would've resonated with Mrs C at the time or prevented her from going ahead with the Payment 1.

As a result, I don't think a proportionate response to the apparent risk would've stopped Payment 1 being made and therefore Revolut can't fairly be held responsible for the loss or be required to refund Payment 1.

But when Mrs S made Payment 2, for €10,800 the following day, a more concerning pattern had emerged. It was the second payment identifiably going to a cryptocurrency exchange provider, the amount had doubled in value and was for a significant amount. So, I think it ought reasonably to have been concerned that Mrs S was potentially at risk of financial harm. I don't consider asking broadly the same questions was sufficient here. And it ought to have taken some steps to ensure Mrs S wasn't at risk. It could have done this by directing her to its in-app chat or through having a conversation with her.

#### *What kind of warning should Revolut have provided?*

As mentioned above, I think Revolut, when Mrs S attempted to make Payment 2 ought to have directed Mrs S to its in-app chat or had a conversation with her about the payment she was making.

Mrs S hasn't been able to provide all of the communication between her and the scammer, but from what has been provided there isn't anything to suggest she was coached heavily in any way or told to disregard any warning provided by Revolut. I've also seen no indication that Mrs S expressed any mistrust of Revolut or financial firms in general. I appreciate Mrs S wasn't entirely truthful when providing her answers to the initial questions asked by Revolut, but that isn't to say that Revolut couldn't have asked further questions of Mrs S and probed the circumstances surrounding Payment 2. And I am mindful Mrs S had said that it was for investing in cryptocurrency – so Revolut ought to have directed its questions to Mrs S and it ought to have focused on the potential risk of cryptocurrency investment scams.

Revolut ought to have been in the position whereby it could have asked a series of open questions to Mrs S about the payment and what it was for. And it ought to have been in a position whereby it provided a warning that was specifically about the risk of cryptocurrency investment scams. And I think that such a warning should have addressed the key risks and features of the most common cryptocurrency investment scams.

The warning Revolut ought fairly and reasonably to have provided Mrs S should have highlighted, in clear and understandable terms, the key features of such 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 think a warning covering the key features of cryptocurrency investment scams affecting many customers, but not imposing a level of friction disproportionate to the risk the payment presented, would have been a proportionate and reasonable way for Revolut to have acted in August 2023 to minimise the risk of financial harm to Mrs S.

*If Revolut had provided a warning of the type described, would that have prevented the losses Mrs S suffered from Payment 2?*

I've thought carefully about whether human intervention with a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented any further loss in this case. And on the balance of probabilities, I think it would have.

There were several key hallmarks of common cryptocurrency investment scams present in the circumstances of Mrs S's payments, such as finding the investment through an advertisement on social media, being assisted by a broker / account manager, being asked to download remote access software, and having paid a small initial deposit which had quickly increased in value and then being pressured to invest more.

There's no evidence to suggest Mrs S was asked, or agreed to, disregard any warning provided by Revolut. In addition, Mrs S did not receive any specific warnings from her other banking provider (from which the money originated) when she transferred money to Revolut – so there's no evidence she ignored a specific and tailored warning.

On the balance of probabilities, if Revolut had asked open and probing questions of Mrs S and provided her with an impactful warning 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. She could have paused and looked more closely into cryptocurrency investment scams. I'm satisfied that a timely human intervention through its in-app chat with a clear warning provided would very likely have caused her to do so, revealing the scam and preventing her subsequent losses.

*Is it fair and reasonable for Revolut to be held responsible for Mrs S's loss?*

In reaching my decision about what is fair and reasonable, I have taken into account that Mrs S sent funds from another bank to Revolut, and then from Revolut to her own cryptocurrency account to enable the purchase of cryptocurrency, 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.

I have carefully considered Revolut's view that in a multi-stage fraud, a complaint should be properly considered only against either the firm that is a) the 'point of loss' – the last point at which the money (or cryptocurrency) remains under the victim's control; or b) the origin of the funds – that is the account in which the funds were prior to the scam commencing. It says it is (in this case and others) merely an intermediate link – being neither the origin of the funds nor the point of loss and it is therefore irrational to hold it responsible for any loss.

In reaching my decision, I have taken into account that the payments were made to another financial business (a cryptocurrency exchange) and that the payments that funded the scam were made from another account at a regulated financial business.

But as I've set out above, I think that Revolut still should have recognised that Mrs S might have been at risk of financial harm from fraud when she made Payment 2, and in those circumstances Revolut should have made further enquiries with Mrs S about the payment before processing it. If it had done that, I am satisfied it would have prevented the losses Mrs S 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 S's own cryptocurrency exchange account does not alter that fact and I think Revolut can fairly be held responsible for Mrs S'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 S 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 she could instead, or in addition, have sought to complain against those firms. But Mrs S has not chosen to do that and ultimately, I cannot compel her to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mrs S's compensation in circumstances where: she has only complained about one respondent from which she is entitled to recover her 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 S's loss from Payment 2 onwards (subject to a deduction for Mrs S's own contribution which I will consider below).

#### *Should Mrs S bear any responsibility for her losses?*

There is a general principle that consumers must take responsibility for their decisions, and I am mindful of the law relating to contributory negligence and the impact a finding of contributory negligence may have to reduce the damages recoverable by a claimant in court proceedings.

I have duly considered whether Mrs S should bear some responsibility by way of contributory negligence, and I'm satisfied she should in the circumstances of this case.

Overall, I consider there to have been enough warning signs that Mrs S was being scammed, which she does not appear to have reasonably acknowledged or acted upon.

Mrs S came across the advert through social media. The contact from here on was seemingly mostly through a messaging app – which to my mind doesn't seem in line with how a legitimate investment firm would communicate. And Mrs S doesn't seem to have been provided, or hasn't provided this service, with any formal contract that she entered into – setting out the terms of any investment arrangement between the two parties. I appreciate Mrs S advised V communicated in her native language and built a rapport – but I don't think that in and of itself means Mrs S ought not to have been aware that things might not be as they seem.

I say this because Mrs S had seemingly been told that she could receive good profits and within a short space of time. I note that the communication Mrs S received on 22 August 2023 indicated her withdrawal was for around \$77,000 – so she had apparently doubled her money (approximately) and within the space of a week. I think it is likely that the returns Mrs S was advised could be achieved from the outset were simply too good to be true. I can't see that Mrs S questioned how such high levels of returns could be realised.

As a result, I'm satisfied Mrs S should've had reasonable cause for concern that things might not be as they seem. But it doesn't appear that she made adequate enquiries into the legitimacy of things or what she was being told. I might understand how in isolation any one of these things may not have prevented Mrs S from proceeding. But when taken collectively I think there were sufficient red flags here that reasonably ought to have led Mrs S to have acted far more cautiously than she did.

So, I think Mrs S did have a role to play in what happened and I think that the amount Revolut should pay to her in compensation should fairly and reasonably be reduced to reflect that role. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

#### Could Revolut have done anything else to recover Mrs S's money?

For completeness, I'll address recovery. The payments were sent to Mrs S's own account with B, were converted into cryptocurrency and then sent to the fraudster. Though Revolut attempted to recover those payments, in these circumstances, it's difficult to see how any recovery from B would have been possible as the funds had already been converted into cryptocurrency and moved on from B.

#### **Putting things right**

For the reasons explained, I uphold this complaint in part and consider Revolut Ltd should:

- refund Mrs S 50% of her loss for Payments 2, 3 and 4 (so €11,415 that being 50% of the sum of Payments 2, 3 and 4)
- pay interest on this amount calculated at 8% simple per year from the date of loss to the date of settlement (if Revolut Ltd deducts tax from this interest, it should provide Mrs S with the appropriate tax deduction certificate).

#### **My final decision**

For the reasons given above and in my provisional decision, I uphold Mrs S's complaint in part. I therefore require Revolut Ltd to pay compensation as I have set out above.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs S to accept or reject my decision before 16 June 2025.

Matthew Horner  
**Ombudsman**