

## The complaint

Mrs T complains that Revolut Ltd ('Revolut') won't refund the money that she lost to an investment scam.

She's being represented by a firm of solicitors. To keep things simple, I'll refer to Mrs T throughout this decision.

## What happened

The background to this complaint is known to both parties, so I won't repeat all the details here. In summary, Mrs T says:

- In February 2023, she came across a social media advert for what she thought was a legitimate company (I'll refer to as R) offering investment opportunities and which was seemingly endorsed by well-known TV personalities. She completed an online form with her contact details and was called immediately by someone claiming to be an 'account manager' (the scammer) at R. She was led to believe he would manage her 'investment account' and make money for her to achieve her financial goals.
- She began to develop what she thought was a genuine relationship with the scammer and, believing she was dealing with an expert who'd be looking after her interests, she was guided through the process of setting up cryptocurrency wallets (with legitimate cryptocurrency platforms) as well as downloading remote access software to allow the scammer to manage her 'investment' on her behalf.
- She had some concerns at first, about some negative reviews she'd seen about R. But these were alleviated when, in support that she was dealing with a legitimate company, she was shown how to withdraw funds to her accounts and the scammer pointed to the ID and KYC checks that were carried out. To make the scam more convincing, she was also given access to what looked like a genuine 'investment platform'; was shown a document apparently to demonstrate that R was registered with Companies House; and was provided with investment information and 'contracts' which again looked legitimate.
- An initial 'investment' of £210 was paid in March 2023 from an account Mrs T held with another bank. And when she saw this 'investment' was slowly increasing, she was persuaded by the scammer she could make more money if she invested more heavily. All further payments for 'investment' were sent from her newly opened Revolut account which the scammer had helped her set up (in March 2023) as part of the scam. In June 2023, she realised she'd been scammed when she was unable to withdraw her money and the scammer told her she needed to pay more for that to happen.

Below are the transactions I've considered as part of this complaint. To note, before issuing this decision we made further enquiries of Mrs T. This included asking for further evidence of withdrawals made as part of the scam. More withdrawals have come to light – which were not considered in the Investigator's outcome – and I've included them in the table below (*in italics*) as they're relevant to my decision. Most of these were withdrawn from Mrs T's cryptocurrency platforms and paid directly to her accounts with other banks ('A' and 'B').

	Date	Time	Type	Payee	Amount
	07-Mar-23		Withdrawal	Mrs T – Revolut	£40.26
1	08-Mar-23	11:41	Card payment	Binance	£1,000
2	13-Mar-23	09:29	Card payment	Binance	£2,900
	12-Apr-23		Withdrawal	Mrs T – bank A	£9.82
	12-Apr-23		Withdrawal	Mrs T – bank A	£785.49
3	24-Apr-23	20:07	Card payment	Binance	£1,000
4	24-Apr-23	20:14	Card payment	Binance	£3,000
5	24-Apr-23	20:16	Card payment	Binance	£3,000
6	24-Apr-23	20:17	Card payment	Binance	£3,000
	09-May-23		Withdrawal	Mrs T - bank A	£1,186.26
7	15-May-23	13:22	Card payment	Binance	£5,000
8	15-May-23	13:23	Card payment	Binance	£5,000
9	15-May-23	13:25	Card payment	Binance	£6,000
10	15-May-23	13:25	Card payment	Binance	£6,000
11	25-May-23	14:15	Card payment	Cro	£35
	25-May-23		Withdrawal	Mrs T – bank B	£2,374.36

The scam was reported to Revolut in July 2023. A complaint was later raised and referred to our Service. Our Investigator considered it and upheld it.

In summary, she thought there was enough about Payment 4 (as above) for Revolut to have intervened and provided Mrs T with a tailored warning covering off the key features of cryptocurrency investment scams. She found that if Revolut had provided such a warning, then this would have likely unravelled the scam – and Mrs T’s further losses would have been prevented. She said Revolut should therefore refund Payments 4-11 plus interest. She didn’t think Mrs T had acted unreasonably during the scam such that there should be a deduction for contributory negligence from the compensation she’d recommended.

Mrs T accepted the Investigator’s outcome. In more recent submissions she also said the money she was able to withdraw from the scam can be deducted from her claim. Revolut disagreed with the Investigator’s outcome and made further representations. In summary:

- Revolut is bound by contract, applicable regulations, and the common law to execute Mrs T’s valid payment instructions. The transactions were authorised by Mrs T and, under the relevant regulations, it must process payments promptly.
- It recognises its obligations to put adequate procedures to counter the risk that it may be used to further financial crime (and has such systems in place) but that duty doesn’t go as far as requiring Revolut to create friction against card payments which are meant to be performed with immediate effect as per the card network’s system.
- The duty to execute valid payment instructions doesn’t require Revolut to assess the commercial wisdom or potential loss of a proposed transaction. This was confirmed by the Supreme Court in the case of *Philipp v Barclays Bank UK plc [2023] UKSC 25*. In this case, there was no uncertainty as to the validity of Mrs T’s instructions and any delay by Revolut to execute payments would have amounted to a breach of its duty to Mrs T.
- The payments from Mrs T’s Revolut account don’t fit either the definition of an APP fraud or fall under the Lending Standards Board Contingent Reimbursement Model (‘CRM

Code') – of which it is not a signatory. It shouldn't be required to refund 'self-to-self' transactions, where it is only an intermediate link in a chain of transactions.

- It shouldn't be responsible for the losses simply because the third party sits outside the Financial Ombudsman Service's jurisdiction, either because the firm isn't authorised, or the product isn't regulated. There's no rational explanation as to why the Financial Ombudsman Service considers Revolut should be responsible for all, most, or 50% of a customer's loss in such scenarios where the relevant transaction is 'self-to-self'.

## **Provisional decision**

I issued my provisional decision on this case on 5 February 2025. I set out the background as above and explained I intended to uphold this complaint but that the redress I planned to award was different to what the Investigator recommended. I provided the following reasons:

*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 (the 2017 regulations) and the terms and conditions of the customer's account. And, as the Supreme Court 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 T 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 with Mrs T to refuse payments in certain circumstances, including to comply with regulatory requirements such as the Financial Conduct Authority's (FCA) Principle for Businesses 6, which required financial services firms to pay due regard to the interests of their customers and treat them fairly.*

*I'm 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'm 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, at the time of these payments, 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'm 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;<sup>1</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.*

*For example, it's my understanding that, in March 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'm 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)<sup>2</sup>.*
- 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".*

---

<sup>1</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>2</sup> 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.

- *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 don't suggest Revolut ought to have had concerns about money laundering or financing terrorism here. I nevertheless consider these requirements 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 (Revolut was not a signatory), but the standards and expectations it referred to represent 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 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 that, at the time of these payments, 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;*

---

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

- *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 and 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'm required to take into account the matters set out at DISP 3.6.4R when deciding what is fair and reasonable, I'm satisfied that to comply with the regulatory requirements that were in place in March 2023, Revolut should in any event have taken these steps.*

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

*It isn't in dispute Mrs T was the victim of a cruel scam here, nor that she authorised the card payments to her cryptocurrency platforms (from where her funds were subsequently sent and lost to the scammer).*

*I'm aware that cryptocurrency platforms generally stipulate that the card used to purchase cryptocurrency on their platform 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 most of the disputed payments would be credited to a cryptocurrency wallet held in Mrs T's name.*

*But by March 2023, when the disputed payments began, 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<sup>4</sup>. And by March 2023, further restrictions were in place<sup>5</sup>. 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. I'm also mindful 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*

---

<sup>4</sup> See, for example, Santander's limit of £1,000 per transaction and £3,000 in any 30-day rolling period introduced in November 2022.

NatWest Group, Barclays, Lloyds Banking Group and Santander had all introduced some restrictions on specific cryptocurrency exchanges by August 2021

<sup>5</sup> In March 2023, both Nationwide and HSBC introduced similar restrictions to those introduced by Santander in November 2022.

*numerous examples of customers being directed by fraudsters to use Revolut accounts in order to facilitate the movement of a fraud victim's money from their high street bank to a cryptocurrency provider, a fact Revolut is aware of.*

*So, taking into account all of the above, I'm satisfied that by the end of 2022, prior to Mrs T's payments from March 2023, Revolut ought, fairly and reasonably, to have recognised 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 customer's own name. And, considering all of the above, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think the fact the disputed payments in this case were going to an account in Mrs T's own name should have led Revolut to believe there wasn't a risk of fraud.*

*I've therefore gone on to consider, taking account of what Revolut knew about the payments, at what point, if any, it ought to have identified Mrs T might be at a heightened risk of fraud that merited its intervention.*

*Like the investigator, I don't think there was enough about Payments 1-3 that ought to have caused Revolut concern to the extent that it should have intervened on suspicion that Mrs T was at a heightened risk of fraud – considering also the payment amounts, the timing of the payments, as well as the fact the account was newly opened so there was limited material account history on which to assess the level of risk presented by those payments.*

*By Payment 4, however, a pattern had begun to emerge. It was higher than any earlier payments and marked an increase in the daily spend. It was also made within minutes of an earlier cryptocurrency related transaction to the same payee on the same day. In my view, given these factors and what Revolut knew about the destination of Payment 4, there was enough for it to have been concerned Mrs T might be at a heightened risk of financial harm from fraud. And, in line with good industry practice and regulatory requirements, I consider it's fair and reasonable to conclude Revolut should have warned Mrs T before that payment went ahead.*

#### *What did Revolut do to warn Mrs T?*

*Revolut has said the account was newly opened so there was no history it could have considered to determine normal activity; the payments were in line with Mrs T's stated account opening purpose; the initial payment of £1,000 established the account purpose and there was no reason for it to suspect that subsequent activity was unusual. It hasn't suggested Mrs T was provided with any scam warnings on any of her payments.*

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

*I've thought carefully about what a proportionate warning in light of the risk presented by Payment 4 would have been in the 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 the payment was made.*

*Taking that into account, I think Revolut ought to, when Mrs T attempted to make Payment 4, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider, have provided a written warning that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. In doing so, I recognise it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency scam without significantly losing impact.*

*So, at that point in time, I think such a warning should have addressed the key risks and features of the most common cryptocurrency scams – cryptocurrency investment scams. The warning Revolut ought, fairly and reasonably, to have provided should have highlighted, in clear and understandable terms, the key features of common cryptocurrency investment scams – for example, referring to an advertisement on social media, promoted by a celebrity or public figure; the involvement of an ‘account manager’, ‘broker’ or ‘trader’, acting on their behalf; the use of remote access software; a small deposit quickly increasing in value; the prospect of unrealistic returns.*

*I again realise 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 T by covering the key features of scams affecting many customers while not imposing a level of friction disproportionate to the level of risk the payment presented.*

*If Revolut had provided a warning of the type described, would that have prevented the losses Mrs T suffered from Payment 4?*

*I’ve thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented Mrs T’s further losses 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 surrounding Mrs T’s payments, such as finding the investment on social media, through an advertisement endorsed by TV celebrities; being assisted by an ‘account manager’; and being asked to download remote access software so they could manage her investment. And I note that, on the day Payment 4 was made, the scammer provided Mrs T with a ‘contract’ guaranteeing returns on her investment with no risk to capital.*

*I’ve also seen the messages Mrs T exchanged with the scammer. I note she’d also spoken to the fraudster and I can’t know for sure what was said in those conversations. But I’ve not found anything in the messages to suggest Mrs T was asked, or agreed to, disregard any warning from Revolut. I’ve found no indication she expressed mistrust of Revolut or financial firms in general. And, following our enquiries, I’ve not found anything to suggest Mrs T was provided with (or ignored) relevant warnings from the firm from which the money to fund the scam originated. I’ve also thought carefully about the fact Mrs T says she’d developed a level of trust in the scammer and that they were able to reassure her she was dealing with a genuine company. But I don’t consider the circumstances (or the relationship) were such that Revolut would have likely found it difficult to break the ‘spell’ through an effective warning.*

*In other words, on balance, I’m not persuaded Mrs T was so taken in by the fraudster to the extent she wouldn’t have paid attention to a warning from Revolut. And, again on balance, if Revolut had shown Mrs T an impactful warning (like the one I’ve described) that highlighted the key warning signs of a cryptocurrency scam (many of which were relevant to her situation at the time) and how she could protect herself from the risk of fraud, I believe it would have resonated with her. She could, for example, have paused and made further enquiries into cryptocurrency scams and she could have looked more closely into R and whether it was regulated in the UK or abroad. All things considered, I think it’s likely a timely warning from Revolut would have caused Mrs T to stop and prevented her further losses.*

*Is it fair and reasonable for Revolut to be held responsible for Mrs T’s loss?*

*In reaching my decision about what’s fair and reasonable, I’ve taken into account that Mrs T first moved money from her account with another bank, to her account with Revolut, and then to cryptocurrency platforms in her name before the funds were lost to the scam.*



*But, as I've set out above, I think Revolut still should have recognised Mrs T might have been at risk of fraud when she made Payment 4 and that, in those circumstances, it should have declined the payment and provided an impactful warning. If it had taken those steps, I think it would have prevented Mrs T's further losses. The fact that the money used to fund the scam came from elsewhere and/or wasn't lost at the point it was transferred to Mrs T's own account does not alter that fact. And I think Revolut can fairly be held responsible for Mrs T's loss in such circumstances. I don't think there is any point of law or principle that says 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 T has only complained against Revolut. I accept it's possible other firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, and Mrs T could instead, or in addition, have sought to complain against those firms. But Mrs T has not chosen to do that and, ultimately, I can't compel her to. In those circumstances, I can only make an award against Revolut.*

*I'm also not persuaded it'd be fair to reduce Mrs T's compensation in circumstances where she's only complained about one respondent from which she's entitled to recover her losses in full; hasn't complained against the other firm (and so is unlikely to recover any amounts apportioned to that firm); and where it's 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've set out above, I'm satisfied it would be fair to hold Revolut responsible for Mrs T's losses from Payment 4 (taking account of any withdrawals Mrs T was able to make and subject to a deduction for Mrs T's own contribution which I'll consider below).*

*For completeness, I realise Mrs T's card payments didn't fall within the scope of the CRM code and I don't seek to treat Revolut as if it were a signatory either. I note the comments that the Payment Services Regulator's mandatory reimbursement scheme wouldn't require Revolut to reimburse Mrs T here. But I'm not persuaded either of these things mean I can't consider whether Revolut failed to act fairly and reasonably in this case. I've given my reasons for finding Revolut should have done more to protect Mrs T from the risk of fraud and that, if it had, it's likely she wouldn't have lost more money. I'm satisfied it'd be fair to hold Revolut responsible for part of Mrs T's losses in those circumstances.*

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

*In considering this point, I've taken into account what the law says about contributory negligence as well as what's fair and reasonable in the circumstances of this complaint.*

*As I referred to above, the Investigator upheld Mrs T's complaint and thought that Revolut should refund Payments 4-11. She didn't think Mrs T had acted unreasonably during the scam such that there should be a deduction for contributory negligence. She noted Mrs T was inexperienced and that, although she'd seen some concerning reviews, it was understandable why she was reassured by the withdrawals she was able to make.*

*I recognise there were aspects to the scam that would have appeared convincing. I again note Mrs T says she found the opportunity through an advert seemingly endorsed by well-known TV personalities; was shown graphs and 'investment information'; and was given access to an 'investment platform' which looked convincing. I can understand how all this would have led her to believe she was dealing with a genuine company.*

*I've also thought about the significance of Mrs T's comments that she saw some negative reviews about R but was reassured by the ID/KYC checks carried out and ability to make withdrawals. While she may not recall specifically what those reviews said at the time, my own searches indicate they were mostly because those individuals had experienced a lack of communication and difficulties in withdrawing funds from R. I don't discount the negative reviews entirely. But, given their content and in the context that Mrs T had been able to make withdrawals, I don't think their existence alone is enough to say Mrs T contributed to her losses by continuing to make payments despite her initial concerns. I'll add here that many positive reviews about R had been posted at the relevant time as well.*

*I do however think Mrs T should have been more cautious and done more to check things independently of the scammer at the time the payments in April 2023 came about. I can't overlook, for example, that one of the scammer's 'investment tables' showed Mrs T could make a "risk free" return of 57% on an investment of up to £20,000 over a period of 12 days. It seems this was backed up by a 'protection letter' from the scammer dated 24 April 2023 which "guaranteed" returns on investment and that the capital was "not exposed to any type of risk". I can also see that, in May 2023, Mrs T was provided with another set of 'investment tables'. This time the "risk free" return was 27% over 3 days. This was again backed up with a 'protection letter' guaranteeing investment returns without "any type of risk" to capital.*

*In submissions to our Service, Mrs T said that the profits generated always seemed "realistic and reasonable". But, in my view, Mrs T should have recognised a guarantee of returns and "risk-free" trading as a significant red flag. They were simply too good to be true. I think this should, despite the other convincing aspects, have put her on notice that who she was dealing with might not be genuine. I'm not convinced it was reasonable for her to proceed with her payments without doing more to verify the information she was given. And I think if she'd carried out sufficient checks independently of the scammer (as would reasonably be expected in the circumstances) she'd have likely found, for example, genuine investment firms aren't usually found on social media and are highly unlikely to provide promises or guarantees such as the ones she was given. I'm also mindful that, when Mrs T did check (independently of the scammer) and contacted one of her cryptocurrency platforms to question what she'd been told, she was told she was likely dealing with a scammer.*

*In the circumstances, weighing up the role both parties to the case played in what happened, I think liability for the losses should fairly and reasonably be shared equally and the refund payable by Revolut reduced by 50%.*

#### *Could Revolut have done anything to recover Mrs T's money?*

*All the disputed payments were card payments to Mrs T's cryptocurrency providers. Mrs T then sent and lost that cryptocurrency to the scammer. I'm satisfied there was little Revolut could have done to recover those funds. In addition, I don't consider a chargeback would have had any prospect of success given there's no dispute Mrs T's cryptocurrency providers, provided her with the cryptocurrency, which she subsequently sent to the scammer.*

#### *Putting things right*

*For the reasons I've given, I'm minded to uphold this complaint and intend directing Revolut Ltd to:*

- Refund the payments Mrs T lost to the scam from (and including) Payment 4 onwards, less any withdrawals she received during that time.*

- *Reduce this amount by 50% in recognition of Mrs T's contributory negligence towards her loss.*
- *Pay 8% simple interest per year on this amount, calculated from the date of the payments to the date of settlement, minus any tax lawfully deductible.*

### **Responses to provisional decision**

I invited further comments and evidence from both parties. I provided a deadline for these and said that, unless the new information changes my mind, my final decision would likely be along the lines set out in my provisional decision. Revolut accepted my provisional decision. Mrs T responded with additional comments for me to consider. In summary:

- She accepts the decision to uphold. But is disappointed with the 50% reduction. The scam employed clever tactics, gaining her trust through assurances of transparency, accountability and reliability. She's still processing the trauma and disappointment of being duped by a sophisticated scam. She was vigilant at the time as large amounts were not deposited immediately. She reviewed the account for a few weeks to see if the claims were true before depositing a large amount of money. The account grew every time she traded which made her believe it was a wise decision to invest.
- The KYC process and the contracts drawn up made the scam appear legitimate. The details presented also matched with those on Companies House. She was under the impression that registered companies undergo checks to prove they're legitimate. She thought she was protected. The reasoning for noting that the scam seemed realistic and reasonable was that the account had been very successful since opening, therefore it was natural to find it realistic as similar claims had been previously achieved.
- She carried out the necessary checks when she was asked to pay more to withdraw the whole account. Once the crypto-platform advised they were fake assets, she made no further payments. There was no suspicious activity before this as all the cryptocurrency was transferred to her trading account and she'd been able to withdraw without issues.
- If Revolut raised a concern regarding the transactions, she wouldn't have made them. As Revolut didn't act with due skill, care and diligence as it was legally obliged to do, she strongly feels she should receive the full amount as recommended by the Investigator. She had no experience or knowledge of cryptocurrency and was led by the fraudster.

Her solicitors also submitted, in summary:

- In respect to the "risk-free" element of the trading contract, Mrs T was an inexperienced trader. She didn't know that the rate of return would be considered unrealistic. However, if Revolut had contacted her and provided the appropriate scam warnings and given full advice as to how investment scams look and feel, the scam would have stopped.
- It's not fair to say further due diligence should have been completed by Mrs T in April 2023 as she had already completed checks and sent payments to the scammer from 7 March 2023 to 13 March 2023. It's not reasonable to expect a lay consumer to second-guess their findings after already completing checks as time goes by, just in case the investment may be a scam. Checks were completed originally and they don't agree that further checks ought to have been done one month later.
- Mrs T cross-checked the details of the investment with what was on Companies House and everything about the investment seemed legitimate. She didn't know that a risk-free

investment was a red flag. However, Revolut could have made her aware of this if it had followed its obligations and duty of care. As experts in fraud, with trained front-line staff, it could have explained how a risk-free promise is indicative of a scam.

- The bar that has been set for due diligence that Mrs T ought to have completed is high for a lay person and inexperienced investor. Mrs T wasn't to know genuine investment firms would not advertise or promote via social media. Many genuine firms use social media as a marketing tool.
- Mrs T acted with caution at first and ensured she was happy with what she saw online on the platform and the performance of her investment before continuing. She started with smaller amounts as a beginner and built her confidence over a number of weeks before deciding to increase her deposits. This sort of careful behaviour should not warrant a 50% deduction in the award to Mrs T who was an innocent victim of fraud.

### **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.

Having done so, I've reached the same conclusions as set out in my provisional decision and for the same reasons.

There is no dispute Mrs T was the victim of a cruel scam and I'm sorry about the impact the whole experience has had on her. I've also already agreed that Revolut ought to have done more to protect her from the risk of fraud – and that, if it had, the scam would, on balance, have been unravelled and Mrs T wouldn't have lost more funds. I don't consider it necessary to detail again my reasons for finding Revolut ought to have warned Mrs T in this case, the type of warning I'd have expected, or the findings around causation (all of which are set out above). But, in such circumstances, it's still important to weigh up the role *both* parties played in what happened when considering where responsibility lies for the losses.

In my provisional decision, I acknowledged the Investigator had found there shouldn't be a deduction for contributory negligence on the basis that Mrs T was an inexperienced investor and had been able to make withdrawals. I also acknowledged there were aspects of the scam that would have appeared convincing. I don't imagine Mrs T thought she was sending money to anything other than a legitimate company. Even so, in my view, there came a point that she ought to have acted more cautiously than she did, for the reasons previously set out, such that she should fairly and reasonably share equal responsibility for her losses.

I understand Mrs T's comments that the scammer made her think she'd made successful trades as a way to entice her into 'investing' more heavily and that she thought the returns seemed realistic as similar claims had played out previously. But I'm not persuaded this means the promises of guaranteed risk-free investment returns (like the ones I've seen here) shouldn't nevertheless have reasonably flagged as concerning and led her to have acted more carefully, whether at the outset or later into the scam. I'd also note, in the initial complaint, in relation to her initial 'investment', Mrs T said: *"The scammer invested the initial \$250...she could see that this deposit was making money...When this money began to slowly increase, the scammer convinced [her] to invest more, claiming that the gains would be far higher, the more money she invested"*. She went on to say: *"[she] continued to make payments to the scammer because her account balance was steadily increasing"*.

I again note the comments that, as an inexperienced investor, Mrs T didn't know the rate of return was unrealistic. But, when assessing Mrs T's actions (or inactions) and whether she was partly to blame for her losses, I'm considering what a reasonable person would be

expected to have done in that position. I still think a risk-free investment return of 57% over a period of 12 days or a risk-free return of 27% over 3 days would strike most people as ‘too good to be true’, despite the other convincing aspects of the scam, and should have caused Mrs T to act more cautiously before making more payments. And I’m still satisfied if Mrs T had carried out sufficient checks *independently* of the scammer at that point (as she later did when she contacted her crypto-platform to question what she’d been told) she’d have likely found information that would have made her realise she was likely falling victim to a scam.

As for the comments that it’s unreasonable to expect an inexperienced customer to carry out more checks, a month after having already completed checks, “*just in case the investment may be a scam*”, I think this misses the point that it was the promises Mrs T was provided with (and the ones in April and May 2023 are the only ones I’ve seen) that I think ought to have caused Mrs T to act more cautiously. In any event, I don’t consider it unreasonable to assess whether circumstances arose for a customer to have developed doubts as to the plausibility of a scam *at any point* in the journey. And I don’t consider it unreasonable to find Mrs T ought to have carried out further checks into what she was being told when presented with information (such as guaranteed risk-free returns at the levels I’ve mentioned) that, in my view, ought to have flagged as concerning, even for an inexperienced investor.

I’m again sorry Mrs T was the victim of a scam. I can understand why she wants to do all she can to recover all the money she’s lost. But I’m satisfied there were red flags that ought to have led to her to carry out more checks, which on balance would have led her to realising she was likely falling victim to a scam. In the circumstances, weighing up the role both parties to the case played in what happened, I’m satisfied liability for the losses should fairly and reasonably be shared equally and the refund payable by Revolut reduced by 50%.

### **Putting things right**

For the reasons I’ve given, I uphold this complaint and direct Revolut Ltd to:

- Refund the payments Mrs T lost to the scam from (and including) Payment 4 onwards, less any withdrawals she received during that time.
- Reduce this amount by 50% in recognition of Mrs T’s contributory negligence towards her loss.
- Pay 8% simple interest per year on this amount, calculated from the date of the payments to the date of settlement, minus any tax lawfully deductible.

### **My final decision**

My final decision is that I uphold this complaint.

Under the rules of the Financial Ombudsman Service, I’m required to ask Mrs T to accept or reject my decision before 26 March 2025.

Thomas Cardia  
**Ombudsman**