DRN-5598985

The complaint

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

Ms T is professionally represented, however, to keep things simple, I'll refer to Ms T throughout my provisional decision.

What happened

The background to this complaint is well known to both parties, so I won't repeat what happened in detail.

In summary, Ms T was browsing social media and found an advert for an investment company, I will call X. Ms T left her contact information via an online data capture form, and received an email from X asking her to make an initial payment of £250, and then she would be contacted by a 'financial advisor' to explain the process in more detail. Ms T made the payment and received the promised call. The advisor appeared very knowledgeable and professional which Ms T tells us made her feel she could trust that X was an expert. X provided Ms T with login details for X's trading platform, which she accessed, and Ms T could see trading on her behalf had already begun.

X informed Ms T that they would be responsible for managing her trades and as Ms T had no previous experience of trading, this was something she welcomed. X then asked Ms T to open a wallet with a well-known cryptocurrency provider, which she duly did.

X explained to Ms T that her profits were completely dependent on how much she was willing to invest. As Ms T saw her initial investment grow more than expected, she decided to move funds from her other bank, I'll refer to as 'C', into her Revolut account and started investing more to capitalise on the opportunity.

Below are the transactions I've considered as part of this complaint. This includes the payments she made from her Revolut account as part of the investment, and the profits she was able to withdraw from her cryptocurrency wallet (*in italics*):

Payment	Date	To	Payment Method	Amount
1	04/01/2023	Binance	Card payment	£2,000
2	18/01/2023	Binance	Card payment	£50
3	19/01/2023	Binance	Card payment	£100
4	24/01/2023	Binance	Card payment	£4,850
	03/02/2023	*Miss T - Revolut*	*Credit in*	*£479.25*

	14/02/2023	*Miss T - Revolut*	*Credit in*	*£50.08*
	02/03/2023	*Miss T - Revolut*	*Credit in*	*£1,204.90*
5	17/03/2023	Binance	Card payment	£13,800
	11/04/2023	*Miss T - Revolut*	*Credit in*	*£2,326.89*
	01/05/2023	*Miss T - Revolut*	*Credit in*	*£1,538.91*
	05/06/2023	*Miss T - Revolut*	*Credit in*	*£1,826.60*
	03/07/2023	*Miss T - Revolut*	*Credit in*	*£3,801.18*
	23/08/2023	*Miss T - Revolut*	*Credit in*	*£908.07*

Ms T invested a total of £20,800 with X, and received credits of £12,135.88, with an outstanding loss of £8,664.12. Ms T said she realised she had been scammed when she was contacted by a representative of X and told due to mismanagement of her funds a large portion of her funds had been lost, and she would need to make a payment of £26,000 as an insurance policy to recover the lost funds.

The scam was reported to Revolut in December 2023 as a complaint. But Revolut declined Ms T's claim for reimbursement and, as a result, Ms T referred her complaint to our service.

Our Investigator looked into things but didn't think that the complaint should be upheld. She said she didn't think payments 1-3 appeared unusual as Ms T had held an account with Revolut for around two years prior to the scam payments and the values involved were not out of character for the way she operated her account. She did think Revolut should have been concerned by payment four and provided Ms T with a tailored written warning about cryptocurrency investment scams as the payment was much higher in value than the previous payments she'd made to the cryptocurrency exchange provider. However, the Investigator went on to say even if a tailored written warning had been provided, she didn't think this would have made a difference as Ms T was able to make significant withdrawals from the investment, which was unusual for a scam, and this would've reassured her that X was a legitimate firm. Ms T had also carried out research online on X before investing but hadn't found anything negative, so the Investigator didn't think a tailored written cryptocurrency investment scam warning would have resonated with Ms T enough to have deterred her from making the payments.

Ms T did not agree and mentioned she wasn't able to withdraw any funds until after payment four was made so if Revolut had intervened at this point, the scam could have been effectively prevented.

The matter was passed to me to decide. I issued a provisional decision on 14 May 2024, and I said:

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 Ms 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 implied terms of its contract with Ms 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;*[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's my understanding during the payments, 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)*[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*

[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.

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[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 (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. 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 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 the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Revolut should fairly and reasonably at the time of these payments:

- *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 financial harm from fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally*

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

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'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 at the time the payments took place, Revolut should in any event have taken these steps.

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

It isn't in dispute that Ms T has fallen victim to a cruel scam here, nor that she authorised the card payments to accounts in her name at a cryptocurrency platform (from which her funds were subsequently sent and lost to the scammer).

Whilst I have set out in detail in this decision the circumstances which led Ms T 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 that time, Revolut had much less information available to it upon which to discern whether any of the payments presented an increased risk that Ms T might be the victim of a scam.

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 Ms T's name.

But by the time 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[4]. And by the time the transactions took place,

[4] 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

further restrictions were in place[5]. 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 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 Ms T's payments, 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 Ms T's own name should have led Revolut to believe there wasn't a risk of fraud.

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

Having looked at the first payment of the scam, I can't fairly say that it would have appeared as unusual or suspicious, considering one of the reasons given at account opening was Crypto, so the purchase of cryptocurrency was not entirely out of character. Payment two and Payment three were made two weeks later and were very low in value; in keeping with the previous payment Ms T had made to the cryptocurrency provider, so, I don't think Revolut should reasonably have suspected that they might be part of a scam.

Moving onto payment four, this was larger than any other payment that Ms T had made to a cryptocurrency provider before. And given what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider Ms T was at heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements, I am satisfied that it is fair and reasonable to conclude that before allowing payment four to go ahead, Revolut should have provided Ms T with a tailored written warning about cryptocurrency investment scams.

To be clear, I do not suggest that Revolut should provide a warning for every payment made to cryptocurrency. Instead, as I've explained, I think it was a combination of the characteristics of this payment (combined with those which came before it, and the fact the payment went to a cryptocurrency provider) which ought to have prompted a warning.

For the reasons I've set out above I'm satisfied that by January 2023 Revolut should have recognised at a general level that its customers could be at increased risk of

[5] In March 2023, both Nationwide and HSBC introduced similar restrictions to those introduced by Santander in November 2022.

fraud when using its services to purchase cryptocurrency and, therefore, it should have taken appropriate measures to counter that risk to help protect its customers from financial harm from fraud. Such proportionate measures would not ultimately prevent consumers from making payments for legitimate purposes.

What did Revolut do to warn Ms T?

Revolut has explained that as Ms T made the payments using her debit card, she was required to confirm it was her making the payments via 3DS secure. Essentially confirming she wanted to proceed with the payments using her device.

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 four 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 Ms T attempted to make Payment four, knowing (or strongly suspecting) that the payment was going to a cryptocurrency provider and the amounts involved, have provided a written warning that was specifically highlighting the risks and features 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 a 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 Ms 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 tailored warning of the type described, would that have prevented the losses Ms T suffered from Payment four onwards?

I've thought carefully about whether a specific warning covering off the key features of cryptocurrency investment scams would have likely prevented Ms 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 Ms T's payments, such as finding the investment on social media, through an advertisement endorsed by a TV celebrity

and well-known figure; being assisted by an 'account manager' and as her small deposit had quickly rose in value (and more than expected).

I've also seen the messages Ms T exchanged with the scammer. But I've not found anything in the messages to suggest Ms 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 Ms T was provided with (or ignored) relevant warnings from 'C' - in which the money to fund the scam originated.

Therefore, on the balance of probabilities, had Revolut provided Ms T with an impactful warning that gave details about cryptocurrency investment scams and how she could protect herself from the risk of fraud, I'm not persuaded Ms 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 Ms 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 spoken to Revolut about the warning and her circumstances. So, all things considered, I think it's likely a timely warning from Revolut would have caused Ms T to stop and prevented payment four and any further payments from being made.

<u>What about the actions of Ms T's other bank 'C'?</u>

This scam saw Ms T move funds from her main bank, 'C', to Revolut and then eventually onto the scammer. This complaint is about Revolut and it's not appropriate for me to comment here on whether or not 'C' should have identified she was at risk of harm from fraud and whether it reacted proportionately. But to obtain a full picture of what took place, we have contacted 'C' to establish if they attempted any kind of intervention before transferring her money to Revolut and, if so, how this affects my assessment of whether or not she acted reasonably in the circumstances.

'C' has told us no intervention was attempted on any of the transfers Ms T made from it to Revolut to fund the scam. As a result, I don't think Ms T would have been alerted to the fact she could be speaking to a scammer, nor does it change my view about how Revolut should have dealt with this situation and whether she acted reasonably in the circumstances.

<u>Is it fair and reasonable for Revolut to be held responsible for Ms T's loss?</u>

I have carefully considered Revolut's view that they are (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 them responsible for any loss.

I have taken into account that the payments were made to another financial business and that the payments that funded the scam were made from another account at a regulated financial business. But as I've set out in some detail above, Revolut should've recognised Ms T might have been at risk of financial harm from fraud when she made payment four and either moved it to pending or declined it to make further enquiries. If they had taken those steps, I am satisfied they would have prevented the loss Ms T suffered.

As a result, it would be fair to hold Revolut responsible for Ms T's loss from the point of payment four of £4,850 made on 25 January 2023.

Furthermore, I'm aware that Revolut has referenced the CRM code and the PSR's reimbursement scheme for APP scams. However, Revolut is not a signatory of the CRM code, nor would the payments be covered by the PSR's reimbursement scheme – as it wasn't in force when these payments were made, and it isn't retrospective. I've therefore not sought to apply either here. I've explained in some detail the steps Revolut should have taken before allowing the £4,850 payment to leave Ms T's account.

Should Ms T bear any responsibility for her losses?

I've thought about whether Ms T 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 Ms T'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.

I've considered that there were sophisticated aspects to this scam – not least the apparently credible and professional looking platform which showed Ms T her investment growth/profit. I'm also mindful that Ms T spoke with X, and that she says they came across highly professional and knowledgeable about crypto too – thereby reassuring her about the legitimacy of the investment opportunity.

As an inexperienced investor, I think it was understandable that Ms T 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. And so, she relied heavily upon the guidance of X, whom she considered a legitimate investment firm. Ms T also seems to have invested fairly cautiously to begin with, increasing the amounts she invested slowly over several months and the higher payment being made only after she received returns, which would have increased her confidence in the investment opportunity being genuine.

So, taking all this into consideration, while Ms T may have been overly trusting of X, based on the returns she received and the cautious investments she made, 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 upon detecting the £4,850 payment caused Ms T's losses from this point onwards.

Could Revolut have done anything to recover Ms T's money?

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

My provisional decision

For the reasons I've explained, I'm currently minded to uphold this complaint and I intend to direct Revolut Ltd to:

- *Refund payment four and payment five that Ms T made as part of the scam – minus any funds already recovered, which I've calculated as* ***£6,514.12.***

- *pay 8% simple interest* per year, from the respective dates of loss to the date of settlement.*

**If Revolut Ltd deducts tax in relation to the interest element of this award it should provide Ms T with the appropriate tax deduction certificate.*

Revolut responded to say they didn't have anything further to add to the provisional decision.

Ms T confirmed her acceptance.

As both parties have now responded, I can proceed with making my final decision on this complaint.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

In the absence of any further points for my consideration, I see no reason to depart from the above. I therefore remain of the view that Revolut is responsible for the loss Ms T suffered from payment four and five. It follows that I think Revolut should refund £6,514.12 to Ms T and pay 8% simple interest to recognise the loss of use of money she suffered.

My final decision

My final decision is that I uphold this complaint in part. I direct Revolut Ltd to pay Ms T the following:

- Refund payment four and payment five that Ms T made as part of the scam – minus any funds already recovered, which I've calculated as **£6,514.12.**

- pay 8% simple interest* per year, from the respective dates of loss to the date of settlement.

**If Revolut Ltd deducts tax in relation to the interest element of this award it should provide Ms T with the appropriate tax deduction certificate.*

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms T to accept or reject my decision before 1 July 2025.

Israr Ahmed
Ombudsman