DRN-5009746

The complaint

Miss T complains Revolut Ltd ("Revolut") didn't do enough to protect her when she fell victim to a scam.

What happened

Miss T said she saw an investment advert on social media and she clicked a link which directed her to an investment firm, that we now know to be a scam. She said she filled in an application and received a call from the scam company and spoke with someone purporting to be a trading adviser, I'll refer to them as the scammer. After speaking with the scammer, Miss T decided to invest.

Miss T said she made a small initial payment via an account she held with another firm. She told us she was given an account on the scam company's trading platform which showed live trades. Miss T said the scammer helped her set up a cryptocurrency wallet and she installed remote access software which the scammer used to trade on her behalf.

Miss T told her the scammer suggested she invest larger amounts, which she did and she saw her profits increase. She said her funds fell to near zero and the scammer told her to deposit further funds to save the account, which she did. Miss T said when she wasn't able to withdraw her funds, she realised she'd been scammed.

These are the payments Miss T made to the scam from her account via legitimate cryptocurrency exchanges and the scam related credits she received into her account:

Payment	Date of payment instruction	Type of transaction	Amount
1	**13 April 2023**	**Transfer**	**£3.00**
2	**13 April 2023**	**Transfer**	**£3.00**
	13 April 2023	Credit	£70.00
3	**19 April 2023**	**Transfer**	**£1,500.00**
	21 April 2023	Credit	£100.00
	26 April 2023	Credit	£3.00
4	**27 April 2023**	**Card payment**	**£6,076.41**
5	**24 May 2023**	**Card payment**	**£2,471.76**
6	**5 June 2023**	**Card payment**	**£2,502.66**
7	**15 June 2023**	**Transfer**	**£9,500.00**

**I've included two small initial payments Miss T confirmed she made as part of the scam and three credits Miss T received into her account which she's confirmed were scam related. These weren't included in our Investigator's view, and as they came before the point at which they felt Revolut ought to have intervened (27 April 2023) they wouldn't have affected the redress recommended by our Investigator. I've included them for completeness.*

Miss T complained to Revolut, and her complaint wasn't upheld. Unhappy with Revolut's response, Miss T raised the matter with the Financial Ombudsman. One of our Investigators

looked into the complaint and felt Revolut ought to have intervened when she made the payment on 27 April 2023. They felt if it had provided a proportionate intervention, it would have prevented her from making the payment and those that followed. They held Miss T and Revolut equally responsible for her losses and recommended Revolut refund 50% of her losses from the 27 April 2023 payment, with 8% simple interest applied from when the payments were made until the date of settlement.

Miss T accepted the outcome. Revolut didn't agree. In summary, it said:

- The payments were self-to-self whereby Miss T sent the funds to an account in her own name meaning Revolut is an intermediary in the chain of the scam as the source of the funds lost to this scam originated from a firm other than Revolut and were lost further in the chain.
- It said the Financial Ombudsman should consider the actions of other firms in the chain.

As an agreement could not be reached, the complaint has been passed to me for a final decision.

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 broad terms, the starting position at law is that an Electronic Money Institution ("EMI") such as Revolut is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations (in this case the 2017 regulations) and the terms and conditions of the customer's account.

And, as the Supreme Court has recently reiterated in Philipp v Barclays Bank UK PLC, subject to some limited exceptions banks have a contractual duty to make payments in compliance with the customer's instructions.

In that case, the Supreme Court considered the nature and extent of the contractual duties owed by banks to their customers when making payments. Among other things, it said, in summary:

- The starting position is that it is an implied term of any current account contract that, where a customer has authorised and instructed a bank to make a payment, it must carry out the instruction promptly. It is not for the bank to concern itself with the wisdom or risk of its customer's payment decisions.
- At paragraph 114 of the judgment the court noted that express terms of the current account contract may modify or alter that position. In Philipp, the contract permitted Barclays not to follow its consumer's instructions where it reasonably believed the payment instruction was the result of APP fraud; but the court said having the right to decline to carry out an instruction was not the same as being under a legal duty to do so.

In this case, the terms of Revolut's contract with Miss 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 to refuse payments in certain circumstances, including to comply with regulatory requirements such as the Financial Conduct Authority's Principle for Businesses 6, which required financial services firms to pay due regard to the interests of their customers and treat them fairly. I am satisfied that paying due regard to the interests of its customers and treating them fairly meant Revolut should have been on the look-out for the possibility of fraud and refused card payments in some circumstances to carry out further checks. In practice Revolut did in some instances refuse or delay payments at the time where it suspected its customer might be at risk of falling victim to a scam.

I must also take into account that the basis on which I am required to decide complaints is broader than the simple application of contractual terms and the regulatory requirements referenced in those contractual terms. I must determine the complaint by reference to what is, in my opinion, fair and reasonable in all the circumstances of the case (DISP 3.6.1R) taking into account the considerations set out at DISP 3.6.4R.

Whilst the relevant regulations and law (including the law of contract) are both things I must take into account in deciding this complaint, I'm also obliged to take into account regulator's guidance and standards, relevant codes of practice and, where appropriate, what I consider to have been good industry practice at the relevant time: see DISP 3.6.4R. So, in addition to taking into account the legal position created by Revolut's standard contractual terms, I also must have regard to these other matters in reaching my decision.

Looking at what is fair and reasonable on the basis set out at DISP 3.6.4R, I consider that Revolut should in April 2023 have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances.

In reaching the view that Revolut should have been on the look-out for the possibility of fraud and have taken additional steps, or made additional checks, before processing payments in some circumstances, I am mindful that in practice all banks and EMI's like Revolut did in fact seek to take those steps, often by:

- using algorithms to identify transactions presenting an increased risk of fraud;[1]
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system for authorised push payments;
- providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified. For example, it is my understanding that in date, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat).

I am also mindful that:

[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_/

- Electronic Money Institutions like Revolut are required to conduct their business with "due skill, care and diligence" (FCA Principle for Businesses 2), "integrity" (FCA Principle for Businesses 1) and a firm "must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems" (FCA Principle for Businesses 3)[2].

- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the "Financial crime: a guide for firms".

- Regulated firms are required to comply with legal and regulatory anti-money laundering and countering the financing of terrorism requirements. Those requirements include maintaining proportionate and risk-sensitive policies and procedures to identify, assess and manage money laundering risk – for example through customer due-diligence measures and the ongoing monitoring of the business relationship (including through the scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.

- The October 2017, BSI Code3, which a number of banks and trade associations were involved in the development of, recommended firms look to identify and help prevent transactions – particularly unusual or out of character transactions – that could involve fraud or be the result of a scam. Not all firms signed the BSI Code (and Revolut was not a signatory), but the standards and expectations it referred to represented a fair articulation of what was, in my opinion, already good industry practice in October 2017 particularly around fraud prevention, and it remains a starting point for what I consider to be the minimum standards of good industry practice now (regardless of the fact the BSI was withdrawn in 2022).

- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.

- The main card networks, Visa and Mastercard, don't allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain restrictions on their card issuers' right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of

[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.

transaction, such as by location. The network rules did not, however, prevent card issuers from declining particular payment instructions from a customer, based on a perceived risk of fraud that arose from that customer's pattern of usage. So it was open to Revolut to decline card payments where it suspected fraud, as indeed Revolut does in practice (see above).

Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in April 2023 that Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;

- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;

- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment – (as in practice Revolut sometimes does); and

- have been mindful of – among other things – common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, including the use of payments to cryptocurrency accounts as a step to defraud consumers) and the different risks these can present to consumers, when deciding whether to intervene.

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

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

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

Whilst I have set out in some detail in this decision the circumstances which led Miss 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 Miss T might be the victim of a scam.

I'm aware that cryptocurrency exchanges generally stipulate that the card used to purchase cryptocurrency at its exchange must be held in the name of the account holder, as must the account used to receive cash payments from the exchange. Revolut would likely have been aware of this fact too. So, it could have reasonably assumed that the payments made by card would be credited to a cryptocurrency wallet held in Miss T's name.

By April 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[3]. And by April 2023, when these payments took place, further restrictions were in place[4]. 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 Miss T made in April 2023, Revolut ought fairly and reasonably to have recognised that its customers could be at an increased risk of fraud when using its services to purchase cryptocurrency, notwithstanding that the payment would often be made to a cryptocurrency wallet in the consumer's own name.

To be clear, I'm not suggesting as Revolut argues that, as a general principle, Revolut should have more concern about payments being made to a customer's own account than those which are being made to third party payees. As I've set out in some detail above, it is the specific risk associated with cryptocurrency in April 2023 that, in some circumstances, should have caused Revolut to consider transactions to cryptocurrency providers as carrying an increased risk of fraud and the associated harm.

In those circumstances, as a matter of what I consider to have been fair and reasonable, good practice and to comply with regulatory requirements, Revolut should have had appropriate systems for making checks and delivering warnings before it processed such payments. And as I have explained Revolut was also required by the terms of its contract to refuse or delay payments where regulatory requirements meant it needed to carry out further checks.

Taking all of the above into account, and in light of the increase in multi-stage fraud, particularly involving cryptocurrency, I don't think that the fact most of the payments in this case were going to an account held in Miss T's own name should have led Revolut to believe there wasn't a risk of fraud.

---

[3] 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.

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

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 Miss T might be at a heightened risk of fraud that merited its intervention.

I think Revolut should have identified that the first three payments were going to a cryptocurrency provider, but they were low in value, and I don't think Revolut should reasonably have suspected that they might be part of a scam.

However, the payment made on 27 April 2023 was significantly larger in value and given what Revolut knew about the destination of the payment, I think that the circumstances should have led Revolut to consider that Miss T was at a heightened risk of financial harm from fraud. In line with good industry practice and regulatory requirements, I am satisfied that it is fair and reasonable to conclude that Revolut should have warned its customer before this payment went ahead.

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.

Revolut argues that it is unlike high street banks in that it provides cryptocurrency services in addition to its electronic money services. It says that asking it to 'throttle' or apply significant friction to cryptocurrency transactions made through third-party cryptocurrency platforms might amount to anti-competitive behaviour by restricting the choice of its customers to use competitors. As I have explained, I do not suggest that Revolut should apply significant friction to every payment its customers make to cryptocurrency providers. However, for the reasons I've set out above I'm satisfied that by April 2023 Revolut should have recognised at a general level that its customers could be at increased risk of 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 Miss T?

Revolut has confirmed it didn't intervene on any of the payments.

Revolut said Miss T was presented with a *'Transfer Review Warning'* when she first added the new beneficiary as this is shown each time a transfer payment is made to a new beneficiary from an account for the first time. This warning asks if a customer knows and trusts the payee and if they're not sure, not to pay them. It goes on to say fraudsters can impersonate others.

What kind of warning should Revolut have provided?

I've thought carefully about what a proportionate warning in light of the risk presented would be in these circumstances. In doing so, I've taken into account that many payments that look very similar to this one will be entirely genuine. I've given due consideration to Revolut's duty to make payments promptly, as well as what I consider to have been good industry practice at the time this payment was made.

Taking that into account, I think Revolut ought, when Miss T attempted to make the 27 April 2023 payment, knowing that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form) that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022.

In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency scams, without significantly losing impact.

So, at this point in time, I think that 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, 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 recognise that a warning of that kind could not have covered off all scenarios. But I think it would have been a proportionate way for Revolut to minimise the risk of financial harm to Miss T by covering the key features of scams affecting many customers but not imposing a level of friction disproportionate to the risk the payment presented.

If Revolut had provided a warning of the type described, would that have prevented the losses Miss T suffered from 27 April 2023?

I've thought carefully about whether 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 Miss T's payments, such as finding the investment through an advertisement on social media, being assisted by a broker and being asked to download remote access software.

I've also reviewed the conversations between Miss T and the scammers (though I note that Miss T appears to have spoken to the scammer, and I haven't heard those conversations). I've found nothing within those conversations that suggests Miss T was asked, or agreed to, disregard any warning provided by Revolut. I've also seen no indication that Miss T expressed mistrust of Revolut or financial firms in general. Neither do I think that the conversation demonstrates a closeness of relationship that Revolut would have found difficult to counter through a warning.

I've taken into account that Miss T had received modest actual returns at the point of suggested intervention, but the weight of evidence that I've outlined persuades me that Miss T was not so taken in by the fraudsters that she wouldn't have listened to the advice of Revolut.

I've seen some evidence that the firm from which the funds used for the scam appear to have originated may have given a scam warning when Miss T moved £9,500 to Revolut in order to make the final scam related payment. However, this was based on the payment purpose given of *'transfer to own account'*. This warning highlights if a customer has been told their account is at risk and to move their money, it's a scam. This warning didn't resonate with Miss T and I believe that's because she likely wouldn't have thought it applied to her as it's not related to the scam she was falling victim to. Miss T continuing past this warning doesn't negate Revolut's reasonable requirement to provide a tailored warning as outlined above. And the key difference here is that Revolut knew the payment being made on 27 April 2023 was going to a cryptocurrency provider. Something the sending bank is not as likely to have known.

Therefore, on the balance of probabilities, had Revolut provided Miss T 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 the broker before proceeding, as well as making further

enquiries into cryptocurrency scams and whether or not the broker was regulated in the UK or abroad. I'm satisfied that a timely warning to Miss T from Revolut, would very likely have caused her to stop and carry out further research – revealing the scam and preventing her further losses.

Is it fair and reasonable for Revolut to be held responsible for Miss T's loss?

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

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 payment made on 27 April 2023 was made to another financial business (a cryptocurrency exchange) and that the payments that funded the scam were made from other accounts at regulated financial businesses.

But as I've set out in some detail above, I think that Revolut still should have recognised that Miss T might have been at risk of financial harm from fraud when she made the payment, and in those circumstances it should have declined the payment and made further enquiries. If it had taken those steps, I am satisfied it would have prevented the losses Miss T suffered. 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 Miss T's own account does not alter that fact and I think Revolut can fairly be held responsible for her loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

I've also considered that Miss T has only complained against Revolut. I accept that it's *possible* that other firms might also have missed the opportunity to intervene or failed to act fairly and reasonably in some other way, and Miss T could instead, or in addition, have sought to complain against those firms. But Miss T has not chosen to do that and ultimately, I cannot compel her to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce a consumer's compensation in circumstances where: the consumer has only complained about one respondent from which they are entitled to recover their losses in full; has not complained against the other firm (and so is unlikely to recover any amounts apportioned to that firm); and where it is appropriate to hold a business such as Revolut responsible (that could have prevented the loss and is responsible for failing to do so). That isn't, to my mind, wrong in law or irrational but reflects the facts of the case and my view of the fair and reasonable position.

Ultimately, I must consider the complaint that has been referred to me (not those which haven't been or couldn't be referred to me) and for the reasons I have set out above, I am satisfied that it would be fair to hold Revolut responsible for Miss T's loss for the payment on

27 April 2023 and those that followed (subject to a deduction for Miss T's own contribution which I will consider below).

Should Miss 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.

I recognise that, as a layman who claims to have little investment experience, there were aspects to the scam that would have appeared convincing. Miss T was introduced to it through an advert appearing on social media. I haven't seen this particular advert, but I've seen other examples. In my experience, they often appear as paid adverts on social media websites and a reasonable person might expect such adverts to be vetted in some way before being published. Those adverts also can be very convincing – often linking to what appears to be a trusted and familiar news source.

I've also taken into account the provision of the trading platform (which, I understand, used genuine, albeit manipulated, software to demonstrate the apparent success of trades). I know that scammers used the apparent success of early trades and, as in this case, the apparent ability to withdraw funds to encourage increasingly large deposits. I can understand how what might have seemed like taking a chance with a relatively small sum of money snowballed into losing a life changing amount of money.

So I've taken all of that into account when deciding whether it would be fair for the reimbursement due to Miss T to be reduced. I think it should.

For the most part, Miss T communicated with the scammer via messaging apps and phone calls. I've seen very little by way of email communications and it seems the full scam communications haven't been provided by Miss T. She has confirmed she doesn't have anything further she can provide.

From what I've seen Miss T was told her money was insured and she would not lose it. I think this is an unrealistic expectation for any investment and a reasonable customer would expect their capital to be subject to some level of risk when investing. I think Miss T should have recognised that the offer in relation to volatile financial markets was simply too good to be true. I think this should, despite the overall plausibility of the scam, put her on notice that the investment might not be genuine.

Additionally, the phone communication came from several different numbers and at least one from a non-UK number. Given the scammer told Miss T they had offices based in London I would have expected communications from several numbers including overseas to have raised some concern with Miss T at the time. Equally the numbers don't match those within the emails I have seen which would also be cause for concern.

I have also seen from the scam communications that prior to making the final payment Miss T said she felt conned.

I've concluded, on balance, that Revolut can fairly reduce the amount it pays to Miss T because of her role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

I recognise that Miss T did have a role to play in what happened, and it could be argued that she should have had greater awareness than she did that there may be something

suspicious about the investment scam. But I have to balance that against the role that Revolut, an EMI subject to a range of regulatory and other standards, played in failing to intervene. Miss T was taken in by a cruel scam – she was tricked into a course of action by a scammer and her actions must be seen in that light. I do not think it would be fair to suggest that she is mostly to blame for what happened, taking into account Revolut's failure to recognise the risk that she was at financial harm from fraud, and given the extent to which I am satisfied that a business in Revolut's position should have been familiar with a fraud of this type. Overall, I remain satisfied that 50% is a fair deduction to the amount reimbursed in all the circum-stances of the complaint.

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

I've thought about whether there's anything else Revolut could have done to help Miss T — including if it took the steps it should have once it was aware that the payments were the result of fraud.

As some of the transactions were debit card payments, the only option of recovery was via chargeback. But given the payments were made to legitimate cryptocurrency providers, I don't consider they would have had any prospect of success given there's no dispute the cryptocurrency was provided to Miss T and so, I don't think Revolut could've recovered her loss.

The transfers were sent to a known cryptocurrency exchange. In that case the money would have been exchanged into cryptocurrency and it seems that Miss T got the cryptocurrency she paid for and in these cases, there's no real prospect of successful recovery of funds.

My final decision

For the reasons given above, I uphold this complaint in part and direct Revolut Ltd to pay:

- 50% of Miss T's losses from the payment made on 27 April 2023 and those that followed – I calculate this to be £10,275.42.
- Pay 8% simple interest per year on this amount, from the date the payments debited her account, until the date the refund is settled (less any tax lawfully deductible).

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss T to accept or reject my decision before 11 June 2025.

Charlotte Mulvihill
Ombudsman