DRN-5017866

The complaint

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

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

What happened

The background to this complaint is known to both parties. I won't repeat all the details here.

In summary, in September 2023, Miss T came across a social media post she thought was from a friend about his successes in cryptocurrency. She sent a message and was put into contact with someone claiming to work at a company (I'll call 'D'). She later discovered her friend's social media had been hacked and she'd been communicating with a scammer.

The scammer led her to believe that D was a professional company involved with 'crypto-mining'. And believing she was dealing with a financial expert she made three payments, between 18 and 25 September 2023, from her Revolut account to accounts with legitimate crypto-platforms she'd been told to open as part of the process. The first two payments were for 'investment' and things seemed to be going well initially. The third was made after she'd been led to believe she needed to 'upgrade' and pay more money to withdraw her funds.

She realised she'd been scammed when, despite having paid, she was still unable to access her funds, saw that her friend's social media account was inactive, and then discovered that it had been hacked when she contacted her friend through a separate platform. By that time almost £6,000 had been lost to the scam.

Below are the payments I've considered as part of this complaint.

	Date	**Method**	**Payee**	**Amount** (with fees)
1	18-Sep-23	Card payment	Banxa	£404.22
2	19-Sep-23	Card payment	Moonpay	£2,523.79
3	25-Sep-23	Card payment	Moonpay	£3,034.03

The scam was reported to Revolut on 26 September 2023. A complaint was later made and referred to our Service. Our Investigator considered it and upheld it. In brief, she thought that Revolut ought to have had concerns about Payment 3 (above) and taken steps to establish a possible scam risk – and that if it had provided Miss T with a written warning tailored to cryptocurrency investment scams then her further losses would have been prevented. She also thought Miss T contributed to her losses such that the compensation Revolut needs to pay can fairly be reduced by 50%.

Miss T accepted the Investigator's outcome. Revolut didn't. In summary it has said:

- Revolut is bound by contract, applicable regulations, and the common law to execute Miss T's valid payment instructions. The transactions were authorised by Miss T and, under the relevant regulations, it must process payments promptly. The payments were authorised through 3DS. Miss T failed to meet her due diligence obligations. She saw an advert on social media, contacted her friend, and was connected to the fraudster. She failed to evaluate the risks and didn't verify the legitimacy of the payments. There is no evidence that Miss T was vulnerable or incapable of making investment decisions.

- 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 detect and prevent all fraud, particularly for authorised customer instructions. 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 *Philipp v Barclays Bank UK plc [2023].*

- The payments don't fall under the Contingent Reimbursement Model ('CRM Code') of which it's not a signatory. And the new reimbursement rules don't apply. It shouldn't be required to refund 'self-to-self' payments, where it's only an intermediate link and there are typically other authorised banks and financial institutions in the chain which aren't being held liable but had more data than Revolut. There's no rational explanation as to why it should be held responsible for all, most, or 50% of a loss in such scenarios where the transactions are 'self-to-self'.

- The funds were sent from Revolut to Miss T's accounts with legitimate crypto-exchanges. The fraudulent activity didn't occur via Revolut. The type of payments were not out-of-character or unexpected with the typical way its type of accounts are used. Enquiries should be made about any interventions and warnings that Miss T may have received from other sources. It might also be appropriate to inform Miss T that it might be appropriate for her to complain about other respondents.

What I've decided – and why

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

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

In broad terms, the starting position at law is that an Electronic Money Institution ('EMI') such as Revolut is expected to process payments and withdrawals 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 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 wasn't 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 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 of the terms and conditions said:

> *"20. When we will refuse or delay a payment*
> *We must refuse to make a payment or delay a payment (including inbound and outbound payments) in the following circumstances:*
>
> *If legal or regulatory requirements prevent us from making the payment or mean that we need to carry out further checks."*

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

I'm satisfied that, to comply with regulatory requirements (including the Financial Conduct Authority's 'Consumer Duty' (which requires financial services firms to act to deliver good outcomes for their customers) Revolut should, in September 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.

So, Revolut's standard contractual terms produced a result that limited the situations where it could delay or refuse a payment (so far as is relevant here) to those where applicable regulations demanded that it do so, or that it make further checks before proceeding with the payment. In those cases, it became obliged to refuse or delay the payment. And I'm satisfied that those regulatory requirements included adhering to the FCA's Consumer Duty.

The Consumer Duty requires firms to act to deliver good outcomes for consumers.

Whilst the Consumer Duty doesn't mean customers will always be protected from bad outcomes, Revolut was required to act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud. The Consumer Duty is therefore an example of a regulatory requirement that could by virtue of the express terms of the contract and depending on the circumstances, oblige Revolut to refuse or delay a payment notwithstanding the starting position at law described in *Philipp.*

I've taken both the starting position at law and the express terms of Revolut's contract into account when deciding what is fair and reasonable. I'm also mindful that, whilst its terms and conditions referred to both refusal and delay, card payment system rules meant Revolut couldn't in practice delay a card payment. It could only decline ('refuse') it. But 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 in September 2023 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.

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 do 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 that in September 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:

- 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).
- 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

[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_/

scrutiny of transactions undertaken in 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 to be relevant to the consideration of its obligation to monitor its customer's accounts and scrutinise transactions.

- The October 2017, BSI Code[2], which a number of banks and trade associations were involved in developing, 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 wasn't 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. 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).
- Since 31 July 2023, under the FCA's Consumer Duty[3], regulated firms (like Revolut) must act to deliver good outcomes for customers (Principle 12) and must avoid causing foreseeable harm to retail customers (PRIN 2A.2.8R). Avoiding foreseeable harm includes ensuring all aspects of the design, terms, marketing, sale of and support for its products avoid causing foreseeable harm (PRIN 2A.2.10G). One example of foreseeable harm given by the FCA in its final non-handbook guidance on the application of the duty was *"consumers becoming victims to scams relating to their financial products for example, due to a firm's inadequate systems to detect/prevent scams or inadequate processes to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers"[4].*
- Revolut should also have been aware of the increase in multi-stage fraud, particularly involving cryptocurrency[5] 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 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).

---

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

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

[4] The Consumer Duty Finalised Guidance FG 22/5 (Paragraph 5.23)

[5] Keeping abreast of changes in fraudulent practices and responding to these is recognised as key in the battle against financial crime: see, for example, paragraph 4.5 of the BSI Code and PRIN 2A.2.10(4)G.

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, in September 2023, Revolut should:

- have been monitoring accounts and any payments made or received to counter various risks, including preventing fraud and scams;
- have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is particularly so given the increase in sophisticated fraud and scams in recent years, which firms are generally more familiar with than the average customer;
- have acted to avoid causing foreseeable harm to customers, for example by maintaining adequate systems to detect and prevent scams and by ensuring all aspects of its products, including the contractual terms, enabled it to do so;
- in some circumstances, irrespective of the payment channel used, have taken additional steps, or made additional checks, or provided additional warnings, before processing a payment (as in practice Revolut sometimes does); and
- have been mindful of (among other things) common scam scenarios, how the fraudulent practices are evolving (including for example the common use of multi-stage fraud by scammers, and the use of payments to cryptocurrency accounts as a step to defraud) and the different risks these can present to consumers when deciding if 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 September 2023 Revolut should, in any event, have taken these steps.

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

There's no dispute Miss T was scammed, nor that she authorised the card payments to her accounts with legitimate cryptocurrency platforms (from where her funds were lost to the scam). I'm aware 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 the disputed payments would be credited to a cryptocurrency wallet held in her name.

But, by September 2023, 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 buy cryptocurrency using their accounts or increase friction in relation to crypto-related payments, owing to the elevated risk associated with such transactions. By September 2023, further restrictions were in place. This left a smaller number of payment service providers, including Revolut, that allowed customers to use their accounts to buy 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 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 mindful a significant majority of cryptocurrency purchases 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 to facilitate the movement of funds from their high-street bank to a cryptocurrency provider, a fact Revolut is aware of.

So, taking into account all the above, I'm satisfied that by the end of 2022, prior to Miss 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 buy cryptocurrency, notwithstanding that a payment would often be made to a cryptocurrency wallet in the customer's own name. And, considering all 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 Miss T's name should have led Revolut to believe there wasn't a fraud risk.

I agree with the Investigator that there was enough going on by Payment 3 for Revolut to have had concerns that Miss T might be at a heightened risk of financial harm from fraud. The payment was of significant value. A pattern of increased spending was emerging. It was also to a cryptocurrency provider. As I've explained, this is a factor which added to its risk level. I don't suggest that Revolut should apply significant friction to every payment made to cryptocurrency. However, for the reasons I've set out, I'm satisfied that by September 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 it should have taken appropriate measures to counter that risk to help protect its customers from financial harm.

I've therefore thought carefully about what a proportionate warning in light of the payment 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 primary duty to make payments promptly.

As above, the FCA's Consumer Duty was in force when these payments came about and requires firms to act to deliver good outcomes for consumers including acting to avoid foreseeable harm. This, in practice, involves maintaining adequate systems to detect and prevent scams and to design, test, tailor and monitor the effectiveness of scam warnings for customers. I'm also mindful firms like Revolut have had warnings in place for some time and have developed those warnings to recognise the importance of identifying both the specific scam risk in a payment journey and ensuring consumers interact with the warning.

The upshot of all this is that, when these payments were made, I think Revolut should have had systems in place to identify, as far as possible, the actual scam that might be taking place to then enable it to provide more tailored warnings relevant to that scam.

In this case, Revolut ought to have known Payment 3 was to a cryptocurrency provider and its systems ought to have factored that in. It should also have known cryptocurrency scams have become increasingly varied over the years, where fraudsters have progressively turned to this as their preferred way of receiving a victim's money across a range of different scam-types – including 'romance', 'impersonation', and 'investment' scams. And, with this in mind, I think that, by September 2023, it ought to have attempted to pinpoint the potential risk further by, for example, asking a series of simple automated questions designed to narrow down the type of crypto-related scam risk associated with the payment.

We know Miss T was falling victim to a cryptocurrency investment scam. As above, I'd have expected Revolut to have asked a series of simple questions to establish if that was the risk the payment presented. Once that had been established, it should have provided a warning tailored to that risk. And, in this case, such a warning should have highlighted, in clear and

understandable terms, the key aspects of common cryptocurrency investment scams – including, for example, opportunities on social media promoted by a celebrity; the use of an unregulated 'adviser'; the promise of unrealistic returns; and being asked to pay more to withdraw funds.

I realise any such warning relies on the customer answering questions honestly, but I've seen nothing to suggest Miss T wouldn't have done so here. I also recognise a warning of this kind couldn't cover 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 off the key aspects of such scams, affecting many customers, while not imposing a level of friction disproportionate to the payment risk presented.

Would such a warning have made a difference?

I've thought carefully about whether a specific warning covering off the key aspects of cryptocurrency investment scams would have likely prevented Miss 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 of her payments. She had, for example, found the opportunity through social media. She was being assisted by an unregulated 'adviser/mentor'. She had been promised unrealistic returns with zero risk. She was led to believe Payment 3 was required for her to withdraw funds. I've also reviewed the messages Miss T exchanged with the scammer. I've not seen anything to show she'd have ignored warnings from Revolut. Neither do I think she'd developed such a close relationship with the scammer that Revolut would have found difficult to counter with a warning. And, following our enquiries, there's nothing to show Miss T was given any relevant warnings by the firm from which the money originated.

Overall, and on balance, if Revolut had provided her with a warning about the risk of cryptocurrency investment scams and how she could protect herself from that risk, I think it would have resonated with her and led her to have acted more cautiously. She could, for example, have paused and looked more closely into D and whether it was regulated before proceeding, as well as making further enquiries into cryptocurrency scams.

In reaching the view that a warning would have likely given Miss T the perspective she needed, I'm mindful she came across the 'opportunity' after seeing a post she thought was from a friend. I realise she'd have likely taken some comfort from that. At the same time, I can see from her messages to the scammer, that she had some concerns about what she was being asked to do by the time it came to Payment 3. I'm also mindful that when she realised something wasn't quite right she was quick in trying to contact her friend by phone and then through another social media platform about what was happening. I don't think it would have taken much persuasion (that an impactful warning could have provided) to help her see the scam risk and prompt her to make more checks prior to making Payment 3.

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

In reaching my decision about what's fair and reasonable, I've taken into account that Miss 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, Revolut ought to have identified a risk and provided Miss T with a warning before Payment 3 was processed. If it had, I think it would have likely prevented her 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 Miss T's account doesn't alter that fact. And I think Revolut can fairly be held responsible for Miss T's losses 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 considered that Miss T has only complained against Revolut. 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 Miss T could instead, or in addition, have sought to complain against those firms. But Miss T hasn't done that and I can't compel her to. In the circumstances, I can only make an award against Revolut. As noted above, I've nevertheless considered whether any interventions were carried out by the sending bank when deciding what's fair and reasonable in this case – and, again, I've not seen anything to show Miss T was given (and ignored) any warnings relevant to her situation at the time.

I'm also not persuaded it'd be fair to reduce Miss T's compensation in circumstances where she's only complained about one firm from which she's entitled to recover her losses in full; she hasn't complained against other firms (so is unlikely to recover any amounts apportioned to those firms); and where it's appropriate to hold a firm liable (like Revolut) when it 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 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, I'm satisfied it would be fair to hold Revolut responsible for Miss T's losses from Payment 3 (subject to a deduction for Miss T's own contribution which I'll go on to below).

As for Revolut's comments that neither the CRM code or the new reimbursement scheme apply, 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 that Revolut should have done more and that, if it had, it's unlikely Miss T would have lost more money. I'm satisfied it's fair to hold Revolut liable for her losses in those circumstances.

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.

As noted above, the Investigator upheld Miss T's complaint and concluded that the refund payable by Revolut can be reduced by 50% to account for her contributory negligence. Miss T accepted that outcome and I agree with this position. I note, for example, that she was led to believe she could receive quick returns of £9,000 on a £500 investment. And that before Payment 3 came about she was told the returns were 100% guaranteed with zero risk.

I'm satisfied these kinds of promises would strike most people as 'too good to be true' and should have put her on notice that the 'opportunity' might not be genuine. I don't think it was reasonable for her to proceed with payments without doing more to verify the information she was given. And if she'd carried out sufficient checks independently of the scammer (as would reasonably be expected here) she'd have likely found, for example, that genuine investments are highly unlikely to offer returns or guarantees like the ones she was given.

In the circumstances, weighing up the role both parties to the case played in what happened, I agree liability for Miss T's losses should fairly and reasonably be shared equally and the refund payable by Revolut reduced by 50%.

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

All the disputed payments were made to accounts Miss T held with genuine cryptocurrency platforms. Miss T then sent that cryptocurrency to the scammer. I'm satisfied there was little Revolut could have done to recover those funds by the time that the matter was reported. And it's unlikely a chargeback would have had any prospect of success given there's no dispute Miss T was provided with the cryptocurrency she then lost to the scam.

Putting things right

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

- Refund Payment 3 and reduce this amount by 50% in recognition of Miss T's contributory negligence.

- In terms of interest, the starting position is that Revolut Ltd should pay 8% simple per year on the amount above from the date of the payment to the date of settlement, minus any tax lawfully deductible. In this case, although Miss T borrowed that part of the money used to fund the scam from a friend, I think this approach still results in a fair outcome overall considering the amounts involved and the timing of when Miss T says she repaid most of those funds. But if Revolut Ltd wishes to calculate this interest using the exact dates and amounts of repayments, then it can do so and Miss T should, on request, promptly provide it with the relevant information for it to do that.

My final decision

For the reasons I've given, I uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss T to accept or reject my decision before 2 July 2025.

Thomas Cardia
Ombudsman