DRN-5462543

The complaint

Mr S complains that Revolut Ltd won't reimburse him after he fell victim to an impersonation scam.

What happened

On 19 March 2025, I issued my provisional decision on this complaint. I wanted to give both parties a chance to provide any more evidence and arguments before I issued my final decision. That provisional decision forms part of this final decision and is copied below.

The background to this complaint is well known to both parties, so I won't repeat it in detail here. But briefly, Mr S has explained that in July 2023, he received a call from an individual purporting to work for his credit card provider. Unknown to Mr S at the time, this individual was in fact a fraudster.

The fraudster asked Mr S if he had made particular transactions earlier that day, which he confirmed he hadn't. The fraudster asked if Mr S had recently clicked any links sent to his phone and he recalled he had received one regarding rearranging a parcel delivery. The fraudster told Mr S this had been a scam message and his phone may have been hacked. He was asked who else he banked with, and Mr S told the fraudster who his primary current account was with. Mr S was told this banking provider would be alerted and would contact him shortly.

Mr S then received another call from a fraudster purporting to work for his main account provider. Mr S checked the number he was called from online and saw this tallied with the account provider in question. Mr S was told that as his phone had been compromised, he needed to move his money somewhere safer. He was asked which other accounts he held and Mr S advised of these, one of which was Revolut. Mr S was told that as Revolut is based solely online, it is a safer account from hacking and also has the strongest facial recognition, so was told to send his money there. Mr S made account transfers from two other banking providers to his account with Revolut.

The fraudster then asked Mr S if he has any password storage applications on his phone, which he confirmed he did. Mr S was told this was a very serious problem, as the hacker would have access to everything. At this point Mr S has explained he became really worried. He was asked if he held any cryptocurrency accounts, which he confirmed he did. The fraudster told Mr S he would arrange for the cryptocurrency provider to send him new account wallet information by text, and that here, his money would be safe, as cryptocurrency is decentralised and untraceable, but still insured. He was told that the texts he'd receive would contain nothing else, as the hackers were probably aware of everything being received on Mr S' phone. Mr S then received a text message on an existing chain of messages from his cryptocurrency account provider, with details of a new account wallet. Mr S therefore made payments as requested from his Revolut account to the cryptocurrency provider. In total, the following card payments were made:

Date and time of payment	***Payment value***
21/07/2023 22:37	*£4,900*

21/07/2023 22:46	*£4,200*
22/07/2023 00:20	*£,3,800*
22/07/2023 00:22	*£4,500*

Mr S has said that at the time the scam occurred, he was already in a stressful period of his life as he was going through a divorce. Additionally, at the time the calls began, he was putting his children to bed alone and felt stressed by the circumstances. The calls then went on into the early hours of the following morning. He's explained that by first moving his money to accounts owned by him, he felt reassured by what he was doing, rather than the request to move funds to cryptocurrency being immediate.

After calls with the fraudster had ended, Mr S began to feel uneasy about what had happened, and after looking into this further, realised he'd fallen victim to a scam and contacted Revolut to raise a claim.

Revolut considered Mr S' claim but didn't uphold it. It said it provided Mr S with details of the chargeback process, but this wasn't completed, based on not having all the information it needed.

Mr S remained unhappy and referred his complaint to our service. An investigator considered Mr S' complaint and upheld it in part. He said that when Mr S made the first scam payment from his Revolut account, it was sufficiently out of character that he would've expected Revolut to have provided a written warning to Mr S. However, based on the payment Mr S was making, he would've expected this to be based around cryptocurrency investment scams and therefore didn't consider it would've resonated with Mr S.

However when Mr S made the second payment, the investigator thought Revolut ought to have made contact with Mr S to better understand the payments he was making. The investigator considered that had it done so, Mr S would've been honest about what he was doing and the scam would have been uncovered.

However the investigator also thought Mr S could've done more to protect himself. He considered that when Mr S made transfers from one of his accounts to Revolut, he was provided a 'safe account' warning that advised him that a 'bank or any other organisation will never tell you to move money to a new, 'safe' bank account.' It also advised Mr S that 'Fraudsters can make phone calls appear to come from a different number.' The investigator therefore thought Mr S was provided with adequate information to warn him that he was at risk of financial harm.

On this basis, the investigator thought that Mr S and Revolut should share liability for Mr S' losses from his second payment onwards, with Revolut refunding 50% of these payments.

Mr S agreed with the investigator's view but Revolut didn't. In summary it said:

- *These were self-to-self payments, and therefore the scam did not occur on Revolut's platform.*
- *It is irrational and illogical to hold Revolut liable for losses where it is merely an intermediary link.*
- *The Payment Services Regulations 2017 requires Revolut to promptly execute authorized transactions, as these were.*

As Revolut disagreed with the investigator's view, the complaint has been referred to me for a decision.

What I've provisionally 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 Mr S 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 July 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 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 is my understanding that in July 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 am 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 scrutiny of transactions undertaken throughout the course of the relationship). I do not suggest that Revolut ought to have had concerns about money laundering or financing terrorism here, but I nevertheless consider these requirements to be relevant to the consideration of Revolut's obligation to monitor its customer's accounts and scrutinise transactions.*
- *The October 2017, BSI Code*[2]*, which a number of banks and trade associations were*

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

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[3] when considering the scams that its customers might become victim to. Multi-stage fraud involves money passing through more than one account under the consumer's control before being sent to a fraudster. Our service has seen a significant increase in this type of fraud over the past few years – particularly where the immediate destination of funds is a cryptocurrency wallet held in the consumer's own name. And, increasingly, we have seen the use of an EMI (like Revolut) as an intermediate step between a high street bank account and cryptocurrency wallet.*
- *The main card networks, Visa and Mastercard, don't allow for a delay between receipt of a payment instruction and its acceptance: the card issuer has to choose straight away whether to accept or refuse the payment. They also place certain restrictions on their card issuers' right to decline payment instructions. The essential effect of these restrictions is to prevent indiscriminate refusal of whole classes of transaction, such as by location. The network rules did not, however, prevent card issuers from declining particular payment instructions from a customer, based on a perceived risk of fraud that arose from that customer's pattern of usage. So it was open to Revolut to decline card payments where it suspected fraud, as indeed Revolut does in practice (see above).*

Overall, taking into account relevant law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider it fair and reasonable in July 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.*

[3] 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.

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 July 2023, Revolut should in any event have taken these steps.

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

It isn't in dispute that Mr S has fallen victim to a cruel scam here, nor that he authorised the payments he made by card to his cryptocurrency wallet (from where that cryptocurrency was subsequently transferred to the scammer).

Whilst I have set out in this decision the circumstances which led Mr S to make the payments using his 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 Mr S 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 payments would be credited to a cryptocurrency wallet held in Mr S' name.

By July 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[4].

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 Mr S made in July 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.

---

[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.

To be clear, I'm not suggesting 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 July 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. 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 Mr S might be at a heightened risk of fraud that merited its intervention.

I think Revolut should have identified that all payments were going to a cryptocurrency provider (the merchant is a well-known cryptocurrency provider). This type of account activity was out of character for Mr S, having never made cryptocurrency payments from his Revolut account previously. Additionally, they were significantly higher than any other payment Mr S had made on the account in the past 12 months (the next highest being for around £500).

Given what Revolut knew about the destination of the payments, and comparing this to Mr S' typical account activity, I think that when Mr S made the first payment towards the scam, the overall circumstances should have led Revolut to consider that Mr S 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 Revolut should have warned Mr S 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 which ought to have prompted further warning from Revolut.

<u>What did Revolut do to warn Mr S and should it have done more in the circumstances?</u>

Revolut did not provide warnings for any of the payments Mr S made towards the scam, so 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 primary duty to make payments promptly.

Taking that into account, I think Revolut ought, when Mr S attempted to make the first scam payment, knowing that the payment was going to a cryptocurrency provider, to have provided a warning (whether automated or in some other form). As Mr S' payment was being made to a cryptocurrency platform, I think that was the key identifiable scam risk here, given how prevalent they had become by the end of 2022. So I would have expected any warning provided to have covered off cryptocurrency investment scams.

Of course, this wasn't in fact the scam Mr S fell victim to and so, in the circumstances, I don't think it would've had much of an impact on Mr S' decision to proceed with making payments towards the scam. However, when Mr S made the second payment, based on the value of the payments he was making in quick succession and to cryptocurrency (which as I've explained was out of character for the account) I think Revolut ought to have intervened further by contacting Mr S and further questioning him.

If Revolut had provided human intervention, would that have prevented the losses Mr S incurred?

Mr S hasn't indicated that he was being coached by the fraudster in making payments, and I think if Revolut had contacted him and asked what he was doing he would've been honest. Even if the fraudster had tried to coach Mr S at this point, Mr S has indicated he was already becoming suspicious of what the fraudster was telling him to do, so I think it's likely that any further suggestions that Mr S should lie to Revolut would likely have broken the spell at this point.

I therefore think human intervention, be that by in-app chat or phone, would've stopped Mr S from making payment two onwards towards the scam.

Is it fair and reasonable for Revolut to be held responsible for Mr S' loss?

In reaching my decision about what is fair and reasonable, I have taken into account that Mr S passed money to a cryptocurrency wallet in his name. So the funds passed through an additional financial institution before losses were incurred.

I have carefully considered Revolut's view that in a multi-stage fraud, liability for any losses incurred should be recoverable against the financial institution where the loss occurred.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr S might have been at risk of financial harm from fraud when he made the second payment towards the scam, 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 further losses Mr S suffered. The fact that the money wasn't lost at the point it was transferred to cryptocurrency does not alter that fact and I think Revolut can fairly be held responsible for Mr S' loss in such circumstances. I don't think there is any point of law or principle that says that a complaint should only be considered against either the firm that is the origin of the funds or the point of loss.

I've also considered that Mr S has only complained against Revolut about the money he lost from this account. 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 Mr S could instead, or in addition, have sought to complain against those firms. But Mr S has not chosen to do that and ultimately, I cannot compel him to. In those circumstances, I can only make an award against Revolut.

I'm also not persuaded it would be fair to reduce Mr S' compensation in circumstances where Mr S has chosen to only complain about Revolut 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 Mr S' loss from the second payment he made to the scam.

Should Mr S bear any responsibility for his 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 have taken into account what we know about these types of scams – that they can be highly panic-inducing, which is what the fraudster relies on - to not allow the victim time to think clearly. I also have taken into account that Mr S was already experiencing stressful circumstances in his life at the time the scam occurred which may have impacted his ability to think clearly. Mr S has explained that at the beginning of the calls with the fraudster he was putting his children to bed – and by the time he made the final cryptocurrency payment it was gone midnight. So clearly there was an element of fatigue here, both in what he was being instructed to do and from worry. The beginning of the scam was also positioned around the fact that Mr S had opened a phishing hyperlink on his phone – so there was plausibility to what he was being told that his information had been compromised. Additionally, having listened to a follow up call Mr S had with the fraudster, I can see this was clearly a professionally arranged scam and the fraudster was able to navigate all queries Mr S raised effectively.

On balance, I've also considered that Mr S has himself acknowledged that by the time he made payments to Revolut, he was beginning to be suspicious of what he was being asked to do. And I've thought about the warning his other banking provider gave him when moving funds to Revolut. The warning advised that banks will not ask you to move funds to 'safe' accounts – as well as fraudster's abilities to appear to call from other phone numbers.

While I accept this warning related to the scam Mr S was falling victim to, I've thought about the timing and context of this warning. At the time Mr S was provided this warning, he was being told that his account with Revolut was safer than other current accounts – so to move funds simply from one account to another that he had prior ownership and control over. Mr S has therefore explained his concerns were lower at this time, and I can understand why, as there was no apparent danger in what he was being told to do. I can therefore appreciate why Mr S would have paid less heed to a warning at this point when there was little to no perceivable risk in what he was doing.

Additionally, in our experience of these cases, we're aware that the pressure and fear instilled by fraudsters is immense. Customers are led to believe that all the money they own is at risk – as well as their digital footprint – and that there is a time pressure to act. In these circumstances, the provision of a written warning needs to be sufficiently stark to often break the spell. And when I consider that when Mr S saw the warning from his other provider the he hadn't in fact been told to move funds to a 'safe account', I can understand why Mr S moved past these quickly.

While Mr S has confirmed he had higher suspicions when making the payments to cryptocurrency, I don't think it's fair to conclude that by proceeding, he was acting negligently. As explained, Mr S had checked the number he was being called from, the texts he'd received had appeared on genuine text chains and the fraudster he was speaking with, from the subsequent call I've heard, was highly professional and persuasive in explaining what needed to be done. I can therefore understand why, despite having worries, Mr S proceeded on the basis that the legitimacy of the scam overshadowed those suspicions.

All things considered, in the context of Mr S' circumstances, I think the steps he took to protect himself were reasonable and I don't consider he acted with negligence by choosing to proceed with payments under the fraudster's instructions. I therefore don't consider it fair to apply a deduction for contributory negligence.

<u>Could Revolut have done anything else to recover Mr S' money?</u>

I've also thought about whether Revolut could have done more to recover the funds after Mr S reported the fraud.

Payments were made by card to a cryptocurrency provider and that cryptocurrency was sent on 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 cryptocurrency platform performed its given role in providing cryptocurrency in return for payment in sterling.

Overall I think a fair outcome in this complaint is for Revolut to be liable for all losses Mr S incurred from his Revolut account from payment two onwards and for Revolut to reimburse him these losses.

My provisional decision

My provisional decision is that I uphold Mr S' complaint in part. I require Revolut Ltd to reimburse Mr S:

- *Losses incurred from, and including, payment two onwards of the scam (totalling £12,500)*
- *Apply 8% simple interest per year on that amount from the date of each payment to the date of settlement.*

Mr S responded to my provisional decision confirming he accepted it. Revolut confirmed it had nothing further to add.

What I've decided – and why

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

As neither party has raised any new points or objections since my provisional decision, I see no reason to depart from the answer I previously provided. My final decision therefore remains the same as the provisional decision.

My final decision

My final decision is that I uphold Mr S' complaint in part. I require Revolut Ltd to reimburse Mr S:

- Losses incurred from, and including, payment two onwards of the scam (totalling £12,500)
- Apply 8% simple interest per year on that amount from the date of each payment to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 5 May 2025.

Kirsty Upton
Ombudsman