

## The complaint

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

## What happened

The background to this scam is well known to both parties, so I won't repeat it in detail here. But briefly, both parties accept that in around November 2022, Mr L was looking online for ways to invest his money, having received a payment from his retirement fund. Mr L found a firm online who he agreed to invest with, and made a payment of £3,000 from another banking provider towards the investment.

In March 2023, Mr L was told this firm had merged with another firm, which I'll refer to as S. He was told this didn't impact the terms of his investment, although he was later told his investment had crashed due to a natural disaster. Unhappy with how his investment had been handled, S allocated a new account manager to Mr L. Unfortunately unknown to Mr L at the time, both account managers involved were in fact fraudsters and no legitimate investments were being made on Mr L's behalf.

Mr L's new account manager advised Mr L to open an account with Revolut, explaining it would make for faster payments for investment opportunities, which Mr L agreed to do. When opening the account, Mr L confirmed to Revolut that the reason for the account was for 'foreign exchange'. The account manager also told Mr L that they had another 'financial arm' of their business, which I'll refer to as B. Mr L was told that payments would be made to B, and from there, would be added to Mr L's trading account in order for investments to be made. Unknown to Mr L, B is in fact a cryptocurrency platform. Mr L had provided details of temporary Revolut cards to the account manager, and Mr L's funds were being added to this platform, then moved on for the fraudster's gain. Mr L was authorising these payments when prompted to on his Revolut app, unaware that the destination of his funds wasn't his perceived investment platform.

After a few weeks of trading, Mr L requested to make a withdrawal from his trading account. However, Mr L was told he had to be trading for a minimum of one month and needed to have met minimum trade levels, Mr L therefore continued investing further.

Once Mr L believed he had met these requirements, he asked again to withdraw funds. However, his account manager began opening a number of bad trades, whereby all of Mr L's funds appeared to be lost. Mr L said he tried to close these trades himself, but the account manager would reopen them until his investment was entirely lost. At this point Mr L realised he'd been the victim of a scam, and contacted Revolut to raise a claim. In total, Mr L made the following card payments from his Revolut account:

| Date       | Value     |
|------------|-----------|
| 23/03/2023 | £2,000    |
| 29/03/2023 | £9,999    |
| 27/04/2023 | £10,000   |
| 29/04/2023 | £4,997.48 |

|            |           |
|------------|-----------|
| 29/04/2023 | £5,000    |
| 16/05/2023 | £10,000   |
| 16/05/2023 | £9,534.64 |
| 17/05/2023 | £418      |
| 26/05/2023 | £9,991.73 |
| 01/06/2023 | £5,000    |

Mr L also received £917 back in perceived 'commission' from the scam.

Revolut considered Mr L's claim but didn't uphold it. It said it had no rights to log a successful chargeback, as Mr L's funds went to a genuine cryptocurrency platform in return for cryptocurrency. It also said that payments were authenticated, with no signs of an account takeover.

Mr L remained unhappy and referred his complaint to our service. An investigator considered Mr L's complaint and upheld it in part. He considered that while this was a newly opened account with minimal account history to consider, when Mr L made his second card payment, it was a significantly valued payment, and the second to an identifiable cryptocurrency platform, which didn't match with the reason Mr L had provided for opening the account. He considered that based on these factors, Revolut ought to have had concerns that Mr L may be at risk of financial harm from fraud and made further enquiries to Mr L, prior to processing this second payment. The investigator considered that had Revolut done so, the scam would've come to light and Mr L wouldn't have made further payments.

However he also thought Mr L proceeded with payments despite some red flags in the fraudster's requests and communication. He therefore thought a fair outcome was for Mr L and Revolut to share liability for Mr L's losses, from payment two onwards.

Revolut disagreed with the investigator's view. In summary, it said the following:

- For our service to apply reimbursement rules to self-to-self transaction is an error of law and we have irrationally failed to consider this fact.
- It is irrational to hold Revolut liable for losses in circumstances where Revolut is merely an intermediary link – Mr L topped up his Revolut account from his main bank account and transferred those funds to another account in his ownership.
- The fraudulent funds did not originate from Mr L's Revolut account – Mr L lost control of them further in the chain once Revolut's services had concluded.
- There is no regulation that mentions financial institutions have to stop every payment to crypto platforms.

As Revolut disagreed, the complaint has been referred 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 Mr L 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 March 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;<sup>1</sup>
- requiring consumers to provide additional information about the purpose of transactions during the payment authorisation process;
- using the confirmation of payee system for authorised push payments;
- providing increasingly tailored and specific automated warnings, or in some circumstances human intervention, when an increased risk of fraud is identified.

For example, it is my understanding that in March 2023, Revolut, whereby if it identified a scam risk associated with a card payment through its automated systems, could (and sometimes did) initially decline to make that payment, in order to ask some additional questions (for example through its in-app chat).

I 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)<sup>2</sup>.
- Over the years, the FCA, and its predecessor the FSA, have published a series of publications setting out non-exhaustive examples of good and poor practice found when reviewing measures taken by firms to counter financial crime, including various iterations of the *“Financial crime: a guide for firms”*.
- 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<sup>3</sup>, which a number of banks and trade associations were

---

<sup>1</sup> For example, Revolut’s website explains it launched an automated anti-fraud system in August 2018: [https://www.revolut.com/news/revolut\\_unveils\\_new\\_fleet\\_of\\_machine\\_learning\\_technology\\_that\\_has\\_seen\\_a\\_fourfold\\_reduction\\_in\\_card\\_fraud\\_and\\_had\\_offers\\_from\\_banks/](https://www.revolut.com/news/revolut_unveils_new_fleet_of_machine_learning_technology_that_has_seen_a_fourfold_reduction_in_card_fraud_and_had_offers_from_banks/)

<sup>2</sup> Since 31 July 2023 under the FCA’s new Consumer Duty package of measures, banks and other regulated firms must act to deliver good outcomes for customers (Principle 12), but the circumstances of this complaint pre-date the Consumer Duty and so it does not apply.

<sup>3</sup> 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 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 March 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.

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

It isn't in dispute that Mr L 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) even though he wasn't aware at the time that this was the payments' destination.

Whilst I have set out in this decision the circumstances which led Mr L 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 L 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 L's name.

By March 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<sup>4</sup>.

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 L made in March 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.

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

---

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

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

refuse or delay payments where regulatory requirements meant it needed to carry out further checks. So I've gone on to consider, taking into account what Revolut knew about the payments, at what point, if any, it ought to have identified that Mr L 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 known cryptocurrency provider), which conflicted with the purpose Mr L provided for opening his account (foreign exchange). While I don't think the first payment Mr L made was so significant in value that it would've alerted Revolut that Mr L may be at financial risk from fraud, I think that Revolut ought to have had concerns when Mr L made the second payment for £9,999.

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 L before this second payment went ahead.

To be clear, I do not suggest that Revolut should provide a warning for every payment made to cryptocurrency (and as can be seen here, I'm not suggesting Revolut was required to for payment one to this scam). Instead, as I've explained, I think it was a combination of this being a second payment, far higher in value than the first *and* to a cryptocurrency platform, which doesn't reflect the purpose Mr L provided for opening this account, which ought to have prompted a warning.

*What did Revolut do to warn Mr L and should it have done more in the circumstances?*

Revolut did not provide warnings for any of the payments Mr L 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, when Mr L attempted to make the 29 March 2023 payment, knowing that the payment was going to a cryptocurrency provider, I think Revolut ought to have provided, as a minimum, a tailored written that was specifically about the risk of cryptocurrency scams, given how prevalent they had become by the end of 2022. I think it's arguable that even further intervention would've been appropriate here, but I won't consider this further, as I've concluded that a written warning would've sufficed in exposing the scam.

In doing so, I recognise that it would be difficult for such a warning to cover off every permutation and variation of cryptocurrency scam, 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, 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 Mr L 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 cryptocurrency investment scam warning, would that have prevented the losses Mr L incurred?*

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 Mr L's payments, such as the use of an account manager and the initial low deposit quickly increasing in value.

Additionally in this case, Mr L has explained that, due to the nature of how these payments were made, he wasn't even aware that he was making payments to a cryptocurrency wallet – as he believed B, the cryptocurrency platform, was simply an arm of the investment platform. I think even an awareness of the fact he appeared to be making cryptocurrency payments would've been sufficient to give Mr L reason to pause for thought and question this information further.

I've also reviewed the instant messages between Mr L and the fraudster (though I note that Mr L appears to have mostly spoken to the fraudster by phone, and I haven't heard those conversations). I've found nothing within those conversations that suggests Mr L was asked, or agreed to, disregard any warning provided by Revolut. I've also seen no indication that Mr L 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 also reviewed the warnings Mr L was provided with by his other account provider, when transferring funds to his new Revolut account. As Mr L selected payment purposes related to sending funds to an account in his own name, none of the warnings provided by this account included information that would've reasonably put Mr L on notice about this scam.

Therefore, on the balance of probabilities, had Revolut provided Mr L with an impactful warning that gave details about cryptocurrency investment scams and how he could protect himself from the risk of fraud, I believe it would have resonated with him. He 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, which I think in the particular circumstances of this complaint would've uncovered the scam Mr L was falling victim to.



*Is it fair and reasonable for Revolut to be held responsible for Mr L's loss?*

In reaching my decision about what is fair and reasonable, I have taken into account that Mr L, albeit unknowingly, purchased cryptocurrency which credited an e-wallet held in his own name, rather than making a payment directly to the fraudsters. So, the funds passed through an additional financial institution before losses were incurred.

I have carefully considered Revolut's view that it shouldn't be held responsible in circumstances where it considers itself an intermediary link in the scam.

But as I've set out in some detail above, I think that Revolut still should have recognised that Mr L 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 losses Mr L suffered. Whether or not the money was 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 L's loss in such circumstances (although in this case it doesn't appear Mr L had control or much of an awareness of this cryptocurrency account in any event, and therefore it appears the funds *were* lost once they left the Revolut account). In any event, 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 L has only complained to our service 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 L could instead, or in addition, have sought to complain against those firms. But Mr L 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 L's compensation in circumstances where Mr L 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 L's loss from the second successful payment he made to the scam from his Revolut account (subject to a deduction for Mr L's own contribution which I will consider below).

*Should Mr L 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 recognise that there were aspects to this scam that would have appeared convincing. Mr L spoke with his account manager regularly, both by phone and messaging, and had access to a platform where he could see the progress of his investments. Mr L also came across this scam firm via his own internet search, rather than receiving a 'cold call'.

So I've taken all of that into account when deciding whether it would be fair for the reimbursement due to Mr L to be reduced. I think it should.

Mr P has explained that prior to making payments through Revolut towards the scam, he'd made another payment through a different banking provider some months earlier. However these funds were lost entirely due to a 'natural disaster' and Mr L therefore started his investment again when using his Revolut account. While I appreciate all investments come with risks, considering Mr L's earlier funds were lost in their entirety, I think it ought to have prompted Mr L to proceed with caution prior to investing further with this same firm. I accept he made attempts to conduct some research prior to investing, although Mr L doesn't recall if this was mainly through the fraudster's own website – rather than using independent sites.

Mr L has also explained that he had attempted to make a withdrawal earlier on in the scam and had been told he hadn't yet met the minimum levels of trade to do so. As this was an early indication of 'changing goalposts' or unclear trade terms, I think this was another red flag where Mr L could have looked further into what he was being told and question inconsistencies.

Mr L has advised that he wasn't given a specific rate of return of his investment – however it's clear the perceived profits on his 'investments' were quite significant. While I accept profits to investments can vary depending on risk appetite, I think Mr L should have questioned whether these levels of profits may be too good to be true. Therefore, while the overall scam was plausible, I think the above elements ought to have put Mr L on notice that something may be amiss.

I've concluded, on balance, that Revolut can fairly reduce the amount it pays to Mr L because of his role in what happened. Weighing the fault that I've found on both sides, I think a fair deduction is 50%.

*Could Revolut have done anything else to recover Mr L's money?*

I've also thought about whether Revolut could have done more to recover the funds after Mr L 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 Mr L and Revolut to be equally liable for all losses Mr L incurred from his Revolut account and for Revolut to reimburse him 50% of these losses.

## **My final decision**

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

- 50% of losses incurred to the scam from payment two onwards (£32,470.25), with a deduction to this figure to account for the £917 credit received, by apportioning this credit across *all* scam payments and then deducting on those requiring reimbursement (resulting in a refund of £32,025.62)
- 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 L to accept or reject my decision before 29 November 2024.

Kirsty Upton  
**Ombudsman**