

The complaint

Mr C complains that Lloyds Bank PLC won't provide him with a refund when he lost money to a job scam. Mr C is represented in this complaint, but I'll refer to him as it's his complaint.

What happened

The detailed background to this complaint is well known to both parties. So, I'll only provide a brief overview of some of the key events here.

Mr C explains that, following sad family bereavements which impacted upon his support network, he was contacted on a messaging app by a fake recruiter and, due to his retirement on health grounds and his restricted income, he was interested in the commission based remote job that they were promoting with fake Company F.

After speaking to a Company F representative, who sounded professional, Mr C agreed to start a task-based job remotely reviewing hotels and businesses. He was recruited, trained, introduced to co-workers and an account was created for him on a Company F platform, all of which made him think the job was legitimate.

The job appears to have been completing simple review tasks, aimed at boosting search engine optimisation, to earn high commission rates. After completing a set of tasks, subsequent sets attracted high commission but created a negative balance. To be able to continue with the job and earn the high commission Mr C then found it necessary to credit his account by paying Company C more and more money via a crypto exchange.

Mr C paid the scammers' crypto account first from his Firm R account (an Electronic Money Institute {EMI}) and then from his Firm C account (a crypto exchange) after making the following 14 payments from his Lloyds account:

Payment Number	Date	Time	Payment Method	Payee	Amount
1	28/5/25	12.57	Debit card	Mr C's account with Firm R	£250
2	28/5/25	16.17	Debit card	Mr C's account with Firm R	£300
3	28/5/25	17.20	Debit card	Mr C's account with Firm R	£300
4	28/5/25	19.18	Debit card	Mr C's account with Firm C	£100.48
5	28/5/25	20.24	Debit card	Mr C's account with Firm C	£400
6	28/5/25	20.33	Debit card	Mr C's account with Firm C	£400
7	28/5/25	20.54	Debit card	Mr C's account with Firm C	£600
8	29/5/25	15.12	Debit card	Mr C's account with Firm C	£1000.96
9	29/5/25	15.19	Debit card	Mr C's account with Firm C	£450.96
10	29/5/25	15.23	Debit card	Mr C's account with Firm C	£300.96
11	30/5/25	16.50	Faster payment	Mr C's account with Firm C	£1500

12	30/5/25	16.51	Faster payment	Mr C's account with Firm C	£1500
13	30/5/25	16.52	Faster payment	Mr C's account with Firm C	£1500
14	30/5/25	17.08	Debit card	Mr C's account with Firm C	£1,560.87
					£10,164.23

Mr C realised he'd been scammed when he couldn't make a withdrawal, and he was being pressured to borrow money to credit his account.

Mr C contacted Lloyds to complain about their lack of intervention, as the payments should've stood out as unusual, and to claim a refund of his loss together with interest and £300 compensation. However, Lloyds rejected his claim as the payments were made from other accounts in his name.

Mr C brought his complaint to our service and our investigator considered that Lloyds should've intervened on payment 12, with a dynamic automated warning, and that this would've likely unravelled the scam. As she also thought Mr C could've done more to protect himself, she said Lloyds should refund 50% of Mr C's loss from payment 12 together with 8% interest.

However, Lloyds disagree and when requesting an ombudsman decision their points included the following:

- They '*previously evidenced payments Mr C made to Firm R and Firm C prior to the scam and as he had successfully sent payments and hadn't raised these as fraud, understandably we would see the latter payments as lower risk as they were going to accounts held in his own name he had previously sent successfully funds to*'.
- '*Crypto platforms offer genuine and legitimate services to many consumers. Therefore, it would not be fair or reasonable to assume that a larger payment to a cryptocurrency exchange is inherently suspicious, and we should have intervened.*'
- '*It would be inappropriate to assume that all cryptocurrency-related transactions are scams and subject them to additional checks. Such an approach would create unnecessary inconvenience for customers and the bank, require significant operational resources, and could detract from our ability to identify and prevent scams in other areas where risk indicators are more apparent*'.
- They '*can't determine how Mr C would've responded to any questions asked or warnings given*'.
- If they '*had intervened and spoken to him, we must recognise this was an existing wallet and Mr C would have been able to reassure the colleague the wallet was in his name and he had been sending money to the wallet for some time. This would be evidenced by his account activity and therefore it is unlikely we would have needed to probe further*'.

On 3 March 2026, I issued a provisional decision and this is what I said:

I've considered the relevant information about this complaint.

My provisional decision is different to the outcome reached by our investigator. So, I'd like to give both parties an opportunity to respond.

The deadline for both parties to provide any further comments or evidence for me to consider is 17 March 2026. Unless the information changes my mind, my final decision is likely to be along the following lines.

If I don't hear from Mr C, or if they tell me they accept my provisional decision, I may

arrange for the complaint to be closed as resolved without a final 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.

Having done so, my provisional decision is different to our investigator's view. I'm not upholding this complaint and I'll explain why.

I should first say that:

- *I'm persuaded by Mr C's submissions and transactions that a scam has occurred here and I'm very sorry to hear that he has lost a significant amount of money to the cruel scammers.*
- *My role is to independently evaluate the evidence provided by both parties. So, where evidence is incomplete, inconsistent or contradictory, as some of it is here, I must reach my decision on the balance of probabilities – in other words, what I consider most likely to have happened in light of the available evidence and wider circumstances.*
- *I'm satisfied that the APP Scam Reimbursement Rules, introduced by the Payment Systems Regulator in October 2024, for customers who have fallen victim to an APP scam, don't apply here. This is because the payments went to another account under Mr C's control. Also, some were made by card.*
- *Regarding efforts to recover Mr C's loss. As the payments to the scammer were to a crypto exchange and then onto the scammer where they would've been quickly moved, I don't think Lloyds could've been expected to recover the funds.*
- *The Payment Services Regulations 2017 (PSR) and Consumer Duty are relevant here.*

PSR

Under the PSR and in accordance with general banking terms and conditions, Banks should execute an authorised payment instruction without undue delay. The starting position is that liability for an authorised payment rests with the payer, even where they are duped into making that payment.

There's no dispute that Mr C made the payments here, so they are considered authorised. However, in accordance with the law, regulations and good industry practice, banks should be on the look-out for and protect its customers against the risk of fraud and scams so far as is reasonably possible. If it fails to act on information which ought reasonably to alert a prudent banker to potential fraud or financial crime, it might be liable for losses incurred by its customer as a result. Banks do have to strike a balance between the extent to which they intervene in payments to try and prevent fraud and/or financial harm, against the risk of unnecessarily inconveniencing or delaying legitimate transactions.

So, I consider Lloyds should fairly and reasonably:

- *Have been monitoring accounts and any payments made or received to counter various risks such as anti-money laundering and preventing fraud and scams.*
- *Have systems in place to look 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 banks and building societies 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, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

Consumer Duty

Also, from July 2023 Lloyds had to comply with the Financial Conduct Authority's (FCA's) Consumer Duty which required financial services firms to act to deliver good outcomes for their customers. Whilst the Consumer Duty does not mean that customers will always be protected from bad outcomes, Lloyds was required to act to avoid foreseeable harm by, for example, operating adequate systems to detect and prevent fraud.

Lloyds was also required to look out for signs of vulnerability. However, although Mr C has provided information on his vulnerability, I can't see that he'd made Lloyds aware of this and discussed any risks and potential mitigation with them.

With the above in mind the above, I first looked at whether any of Mr C's payments should've been identified as having a heightened risk and triggered automated or human interventions to protect him from financial harm.

Payments 1 to 11

For the following reasons, I also wouldn't have expected Lloyds to have been concerned about any of these payments and therefore triggered an intervention:

- Crypto payments are both legal and common.
- Lloyds process thousands of payments each day and, as mentioned above, they have to strike a balance between the extent to which they intervene in payments to try and prevent fraud and/or financial harm.
- In the months that preceded these payments Mr C regularly made:
 - Transfers to Firm R and for much higher amounts than payments 1 to 3. Also, Firm R are a regulated firm, and Lloyds would have a level of comfort that they would assess the risk with greater information on where the payments were going.
 - Payments to crypto Firm C for amounts up to £250. Also, he received credits from them up to £322.60
- Although I recognise payments 8 and 11 (£1,000.96 and £1,500) were higher amounts than any of the previous payments, and appreciate these were high for Mr C, I don't think these were for particularly high amounts. And Lloyds would've known about another crypto exchange account he held with legitimate Firm K from whom he received a credit of £1900.27.
- Although there were two sequences of same day payments, that were higher than other previous patterns (3 same day Firm C transactions, 2 Firm R transactions), they weren't significantly higher and the combined amounts were relatively low. So, I don't think that there was an obvious scam pattern.

Payment 12

Regarding payment 12, this took Mr C's crypto payments to Firm C on 30 May 2025 to £3,000 and his payments in three days to £6,253.36.

Although Mr C was using crypto exchanges and had approximately six months earlier made a payment for £6,572.18, I think Lloyds should've been aware of the elevated risk of crypto. This is because they would've seen fraud and scams frequently using crypto as a payment method and the financial services regulator issued a warning that customers could lose all their money.

So, I think that it would've been proportionate for them to have implemented their dynamic fraud prevention system to identify the payment reason and issue relevant fraud and scam warnings and education.

Payments 13 and 14

These two payments were also on 30 May 2025, taking Mr C's payments that day to £4,500 (payment 13) and £6,060.87 (payment 14), which meant a high amount of same day payments on crypto payments that have an elevated high risk. Also, the frequency of high payment amounts was unusual and an indicator of a possible scam.

So, if Mr C had continued to make payments after an automated intervention at payment 12, I would've expected Lloyds to have put in place human interventions where a fraud or scam agent could ask probing questions to give relevant warnings and education to detect a fraud or scam.

I can't see that Lloyds did any analysis on payments 12 to 14, considered questioning these payments or have provided sufficient evidence to persuade me that they intervened or that it wasn't proportionate for them to intervene.

If a bank doesn't question payments that might be at risk, then it can't fulfil its duty to protect customers. I'm not saying that means it must check every payment out of its customers' accounts. But here, considering the individual circumstances of this case, I believe it ought to have put in place an intervention to check Mr C wasn't at risk of falling victim to fraud.

I then considered what would've more likely than not have happened if Lloyds put in place a dynamic automated warning at payment 12. To assist me with considering how Mr C would've likely reacted to a job scam warning, I requested information from Firm R. This is because:

- Mr C stopped using Firm R after making the first three payments.*
- Lloyds question how Mr C would've responded.*
- I noticed a messaging app which refers to a possible account suspension from Firm R.*

When considering the information I received from Firm R, I'm not persuaded that a Lloyds warning would've been effective. I say this because the information from Firm R shows that Mr C led them to believe he was making an investment and wasn't being guided.

In addition, although the warnings he received were aimed at investments, some of the messages were strong warnings and / or related to the job scam such as:

- 'This is a high-risk payment'.*
- 'Is this a scam – read carefully before making this high risk payment' (highlighted by an exclamation mark in a red triangle).*
- 'Something doesn't look right'.*
- 'Social media scams – how to stay safe' which included '76% of authorised push payment fraud – when criminals manipulate victims into sending money under false pretences originated online'.*

- ‘Pressure tactics’.
- ‘Common warning signs’ including:
 - ‘High risk returns’, which included, if it sounds too good to be true it probably is’.
 - ‘Exclusive opportunities’, which included, ‘Scammers might claim that an opportunity (such as higher commission) is exclusive or are among the lucky few’.

Furthermore, Mr C indicated he wasn’t being guided by anyone (and was warned that if someone was guiding him, he was being the victim of a scam) and cancelled his payments when Firm R delayed his payments to give him a pause to:

- ‘Get a second opinion’, ‘Research the recipient’, and ‘Stay vigilant on social media.’

I accept that these warnings were not tailored to a job scam. However, when deciding what on balance of probabilities would’ve likely happened, I think it would be remiss of me not to take into account how Mr C responded to these warnings when considering how he would have likely reacted to a job scam warning. I think a reasonable person would have thought carefully had they seen the warnings Mr C saw, regardless of whether it was tailored to a job scam or not. Yet the evidence from Firm R shows that he disregarded their warning, avoided talking to them and stopped using them.

It isn’t possible to know if Mr C’s responses were because he was being coached or because he was under the spell of the scammers and persuaded his bank may interfere or possibly stop his high earnings for very basic tasks. However, based on this Firm R evidence, had Lloyds provided a job scam payment purpose and relevant warning, I’m not persuaded that Mr C would’ve said the payments were for his supposed job. So, I don’t think he would’ve received the relevant job scam warnings and an intervention would’ve prevented his payment 12 loss.

Furthermore, based on the above evidence and Mr C only having submitted partial dialogue between him and the scammers, if Lloyds had put in place human interventions at payment 13 and 14, on balance of probabilities, I’m also not persuaded that these would’ve been effective and Mr C wouldn’t have continued to say he was making an investment. And with his crypto experience and evidence of the crypto activity on his account (including credits), it would’ve been very difficult for a fraud and scam agent to detect his payments were for a job enabling them to unravel the scam and prevent Mr C’s payments.

So, having considered the above and all the information on file, I’m sorry to disappoint Mr C but due to the new evidence, although I think Lloyds should’ve intervened, even if they did, I’m not persuaded that they could’ve prevented his loss.

My provisional decision

For the reasons mentioned above, my provisional decision is not to uphold this complaint against Lloyds Bank PLC.

This is subject to any comments that either Mr C or Lloyds Bank PLC may wish to make. These must be received by 17 March 2026.

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.

Further to my above provisional decision, I only received a response from Mr C which included the following points:

- Firm R's warning information is insufficient to overturn the investigator's decision.
- The automated warnings were weak and evidentially insufficient to help uncover scams.
- He questioned the option choices that he was given by Firm R and whether one was about a job.
- He said that it's unfair to suggest that he wouldn't have listened to more relevant warnings from Lloyds and, if Lloyds had asked questions regarding the payments, they would've discovered that the payments were part of a job opportunity. And if they reached out to him directly, he would've listened and understood he was the victim of a scam, thus preventing him from making further payments.

Before explaining my final decision, I should first say that our investigator issued a view with a recommendation and not a decision. The reason for my involvement is because Lloyds disagreed with the investigator's view. I've summarised their disagreement reasons above and these included the following comment that:

- They couldn't *'determine how Mr C would've responded to any questions asked or warnings given'*.

Due to this reason and my review of the file, including Mr C's telling the scammer that his Firm R account *'is now suspicious'*, I requested information from Firm R on the warnings that they gave Mr C. Firm R then gave a detailed response, and I don't consider their warnings to have been weak.

Due to Mr C's above response to my provisional decision, I requested further information from Firm R on his payment reason selections. They explained that their intelligent fraud prevention system first asked him to select one of the following two options:

- A. *'Yes, I'm investing'*.
- B. *'No, I'm not investing'*.

And Mr C received the warnings – which I've detailed in the above provisional decision – because he selected option A.

Firm R confirmed that if he'd selected option B, which would've been the correct option for a job, he would've received other payment reason choices and then relevant warnings.

It isn't possible to know why Mr C gave the wrong option. Mr C has only submitted partial dialogue between him and the scammer, but this shows a communication where he told the scammer Firm R were *'suspicious'*. This together with the scammer *'teaching'* him to make payments, suggests he may have given the wrong option to Firm R because he was being coached and was under the spell of the scammer and persuaded his bank may interfere or possibly stop his high lucrative earnings.

So, based on Mr C selecting an incorrect payment reason, ignoring some strong warnings and only submitting a partial dialogue (where he talks about Firm R), I'm not persuaded that he wouldn't have tried to circumvent checks if Lloyds put in place an automated warning at payment 12. And, as explained in my provisional decision, I can't safely say that human intervention at payment 13 and 14 would've unravelled the scam, considering Mr C's crypto experience and evidence of the crypto activity on his account (including credits).

Therefore, I'm very sorry to disappoint Mr C but having considered everything again I'm not upholding this complaint against Lloyds Bank Plc.

My final decision

For the reasons mentioned above, including my provisional decision, my final decision is not to uphold this complaint against Lloyds Bank Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr C to accept or reject my decision before 8 May 2026.

Paul Douglas
Ombudsman