

## **The complaint**

X, a limited company, complains Lloyds Bank PLC (“Lloyds”) didn’t do enough to protect it when it fell victim to a scam.

The director of X, Mr D, is bringing the complaint on its behalf via a claims management company. So, in the main, I’ll refer to Mr D throughout.

## **What happened**

Mr D says X received an expected invoice from a company I’ll refer to as E in December 2023, soon after it received an email to say E was changing its bank details and these would be provided shortly. X received the supposed updated bank details for an account in Portugal which we now know was sent by a scammer. Mr D said the invoice from the scammer was identical to the genuine invoice but for the bank details. He told us it even included a number of staff at E copied in as was usual practice. The scammer had used email addresses which very closely resembled that of staff at E.

The invoice was paid by Mr D in a Lloyds branch on 9 January 2024, but it was rejected by the beneficiary bank as the payee name wasn’t correct. Mr D emailed E about this but was unknowingly communicating with the scammer who gave him a new name for the account explaining it was a subsidiary for Euro payments. The payment information was updated with Lloyds, and the payment was made again on 29 January 2024.

The beneficiary bank contacted Lloyds for further checks before processing the payment on 6 and 8 of February 2024. On 14 February 2024 Lloyds spoke with Mr D over the phone. Lloyds say Mr D gave it reassurances during this call he’d verified the change in banking details with E, so it confirmed the payment as genuine to the beneficiary bank. Mr D believes Lloyds should have gone further during this call and suggested he contact E by phone to verify the change in bank details and if it had, he’d have acted on the suggestion and called E to verify the change in bank details which would have uncovered the scam and prevented the loss.

Mr D realised X had been scammed during a routine meeting with E when he requested confirmation the invoice had been paid. It was at this time the difference in the email addresses was noticed and he reported the scam to Lloyds.

Mr D complained to Lloyds, and the complaint wasn’t upheld. Unhappy with Lloyds’ response, the matter was raised with the Financial Ombudsman Service. One of our Investigators looked into the complaint and didn’t uphold it. They felt Lloyds had carried out reasonable checks with Mr D regarding the payment and it had been sufficiently reassured during a call with Mr D that adequate checks had been carried out to verify the change in bank details with E, so it was reasonable for it to process the payment.

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

## What I've decided – and why

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

I'm sorry that X has been scammed and I realise the loss is significant and I don't underestimate the effect this has had on the company. And so, I'd like to reassure Mr D that I've read and considered everything he's said in support of this complaint. But I'll focus my comments on what I think is relevant. If I don't mention any specific point, it's not because I've failed to take it on board and think about it, but because I don't think I need to comment on it to reach what I think is a fair and reasonable outcome. I know this will come as a disappointment to Mr D but having done so, I won't be upholding this complaint. I'll explain why.

In broad terms, the starting position at law is that banks and other payment service providers are expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account.

As the director of X, Mr D authorised the payment in question here – so even though he was tricked into doing so and didn't intend for the money to end up in the hands of a scammer, X is presumed liable in the first instance.

But as a matter of good industry practice, Lloyds should also have taken proactive steps to identify and help prevent transactions – particularly unusual or uncharacteristic transactions – that could involve fraud or be the result of a scam. However, there is a balance to be struck: as while banks and Electronic Money Institutions should be alert to fraud and scams to act in their customers' best interests, they can't reasonably be involved in every transaction.

I've also thought about the Contingent Reimbursement Model and as this is an international payment the code isn't relevant as it doesn't cover international payments.

I've thought about whether Lloyds acted fairly and reasonably in its dealings with Mr D when he made the payment, or whether it should have done more than it did.

I don't know what took place when Mr D initially made the payment in branch or when the payee's name was updated. However, I have a transcript of the call between Mr D and Lloyds which was made prior to the loss which I believe is enough to reach a fair outcome.

I've reviewed the transcript of the call between Lloyds and Mr D. I can see Lloyds asked Mr D how well he knows E and he confirms they've worked together on a project previously. Lloyds ask Mr D if he has verified the change in bank details. Having already given a brief outline of the overall company E comes under, Mr D explained E is restructuring how it operates in Europe and now payments are to go to a Portuguese account. He says the change in bank details has been verified with *'the Americans several times'* and with regard to his steps to verify the bank details Mr D comments, *'I'm quite happy'*.

Lloyds said it was making sure from a security point perspective as *'things can get intercepted'* to which Mr D replies, *'I fully understand, I was pretty nervous when we saw this, spent a bit of time verifying everything'*. From this I'm satisfied Mr D understood that Lloyds was referencing email interception as a possibility, and it seems this was a concern for Mr D prior to this as he says he was nervous initially. So I'm satisfied Mr D was aware he could be falling victim to an email interception/invoice scam.

Lloyds goes on to ask if Mr D had contacted E to make sure the bank details were changed and Mr D explains he's contacted various people at E, including at different offices and in different roles and all had confirmed Mr D was paying the correct account.

Lloyds asks if Mr D checked the beneficiary, and he replies they deal with these people all the time and there's no need to verify them.

It could be argued that Lloyds ought to have done more, as Mr D suggests, given the scam X could have been falling victim to would be an invoice scam but as I've said I think Mr D was already aware this was a possibility prior to making the payment and before his call with Lloyds. And I think even if Lloyds had done more it likely wouldn't have made a difference. I'll explain why.

I've reviewed the communication between Mr D and the scammer and can see it's very similar to genuine communications with E. It also seems the scammer was communicating with E pretending to be X which shows the level of sophistication of the scam. Mr D also made reasonable efforts to verify the change in bank details with E, as far as he was concerned he gained reassurances from more than one member of staff from more than one office. Mr D's testimony is clear, he had no suspicions there was anything untoward going on and X had a trusting relationship with E as this wasn't the first contract the two had. Also, when Lloyds asked if Mr D had checked the beneficiary, he said there was no need. I think this supports the level of trust within the business relationship and that Mr D was satisfied he'd been diligent in his verification of the bank details already.

Additionally, during the call Mr D had with Lloyds he expresses his concerns that the delay in processing the payment will have on the contract and it ends with him raising a complaint about the delay – this hasn't been referred to us. I therefore think, on balance, had Lloyds suggested Mr D carry out any further checks to verify the change in bank details he would have reiterated the checks he'd completed and his desire to have the payment processed without further delay. I'm therefore not persuaded that if Lloyds had done more to highlight the potential scam X could be falling victim to that it would have prevented the loss X suffered.

I'm sorry to disappoint Mr D further, but I've thought carefully about everything that has happened, and with all the circumstances of this complaint in mind I don't think Lloyds needs to refund this money. I realise this means X is out of pocket and I'm really sorry it's lost this money. However, for the reasons I've explained, I don't think I can reasonably uphold this complaint.

### *Recovery*

I've thought about whether there's anything else Lloyds could have done to help X — including if it took the steps it should have once it was aware that the payments were the result of fraud.

Lloyds attempted to recover the funds the same day Mr D reported the scam to it and the beneficiary bank confirmed recovery of the funds wasn't possible. I don't think there's anything more Lloyds could have done to recover X's losses.

### **My final decision**

My final decision is that I do not uphold this complaint against Lloyds Bank PLC.

Under the rules of the Financial Ombudsman Service, I'm required to ask X to accept or reject my decision before 7 August 2025.

Charlotte Mulvihill  
**Ombudsman**