

## **The complaint**

Mr A complains that Lloyds Bank Plc didn't do enough to protect him from the financial harm caused by a job scam, or to help him recover the money once he'd reported the scam to it.

## **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.

On 4 January 2024, Mr A received a WhatsApp message about a job opportunity from someone I'll refer to as "the scammer". When he expressed an interest, the scammer told him about an opportunity to earn money by reviewing films on a platform which I'll refer to as "R". The job required him to pay for tasks using cryptocurrency and at the end of a set of 20-30 'tasks', he would earn commission, and the original deposits would be returned. The scammer told him that a profit was guaranteed.

The scammer told Mr A to open an account with a cryptocurrency exchange which I'll refer to as K and to first purchase cryptocurrency and then load it onto an online wallet. On 26 January 2024, he made two transfers to K totalling £19,000.

In addition to the transactions from Lloyds, Mr A also made three transfers from W totalling £3,502, nine transfers from Bank H to K totalling £64,278, two transfers from Bank N totalling £7,749, and one debit card payment and 38 transfers from R.

Having completed the necessary tasks, Mr A asked the scammer if he could make a withdrawal and was told he'd need to make further payments. He realised he'd been scammed on 13 April 2024 when he ran out of money, he lost contact with the scammer and was unable to access his funds.

Mr A complained to Lloyds with the assistance of a representative who said it should have done more to protect him. But Lloyds refused to refund any of the money he'd lost. It said the payments weren't unusual, and he said he was moving his money to his own account. It also said the Contingent Reimbursement Model (CRM) Code didn't apply to transfers between customer's own accounts and Mr A would need to report the fraud to his other bank.

Mr A wasn't satisfied and so he complained to this service with the assistance of a representative who argued that Lloyds should have intervened on 26 January 2024 when he transferred £9,500 to K. They said Mr A had never purchased cryptocurrency or made such frequent payments to new and different recipients and Lloyds should have been on the lookout for job/task-based scams and asked more robust questions. They said that if it had intervened appropriately, it would have identified that he was falling victim to a scam because he was contacted unexpectedly on WhatsApp, he was asked to open a cryptocurrency account, added to a WhatsApp group with others doing the same job, and required to make deposits to unlock premium tasks to earn commission. In addition, the payments were getting larger and more frequent, which is common in a job scam, he was encouraged to take out loans or borrow from family or friends, he was put under pressure to

make payments, he didn't have an employment contract, and he was told he could double his investment.

They also explained that Mr A believed the opportunity was genuine because he had checked R's website and thought website seemed authentic, there had been a lot of media coverage regarding the move to remote work, and he was added to a WhatsApp group with other employees/freelancers.

Responding to the complaint, Lloyds said the payments weren't out of character and Mr A failed to undertake proper checks such as asking why he needed to make payments when he was supposed to be earning money.

Our investigator didn't think the complaint should be upheld. He thought Lloyds ought to have intervened when Mr A made the first payment because it was a large amount to a cryptocurrency merchant. He thought a proportionate response would have been for it to have called him to discuss the payment, but he didn't think this would have prevented his loss because Mr A didn't listen to advice or warnings from his other banks and he provided misleading answers which prevented them from detecting the scam.

In support of his position, he explained that Mr A provided misleading information to Bank H, which prevented it from detecting the scam. And he went ahead with the payments even though the call handler had given him a detailed explanation about cryptocurrency investment scams.

He also noted that during a call with Bank T on 10 January 2024, Mr A said he was moving funds so that he could purchase a product. He said he wasn't going to purchase cryptocurrency, and he wasn't being encouraged to make the payment. And he became frustrated when the call handler asked him for more information about the purchase. Our investigator commented that Mr A failed to disclose the true nature of the payment which prevented it from detecting the scam.

He also explained that Bank N intervened on 25 January 2024 and Mr A said there was no one instructing him to make the payment. And in a further call on 26 January 2024, he said no one was helping him and that he'd been persuaded to make the payment by friends and family. He was then given a detailed cryptocurrency warning, which he ignored as he went on to make further payments from Bank H and R.

Finally, he noted that Mr A had transferred funds to a legitimate cryptocurrency exchange in his own name and from there he had purchased cryptocurrency and moved it onto a cryptocurrency wallet, so there wouldn't have been any funds to recover. And he didn't think he was entitled to any compensation.

Mr A has asked for his complaint to be reviewed by an Ombudsman. The representative has argued that the fact that Bank H is part of the Lloyds banking group doesn't mean that large cryptocurrency transactions were normal on the Lloyds account and that Lloyds should have intervened when Mr A made the first payment.

### **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.

Having done so, I've reached the same conclusion as our investigator. And for largely the same reasons. I'm sorry to hear that Mr A has been the victim of a cruel scam. I know he

feels strongly about this complaint, and this will come as a disappointment to him, so I'll explain why.

I'm satisfied Mr A 'authorised' the payments for the purposes of the of the Payment Services Regulations 2017 ('the Regulations'), in force at the time. So, although he didn't intend the money to go to scammers, under the Regulations, and under the terms and conditions of his bank account, Mr A is presumed liable for the loss in the first instance.

There's no dispute that this was a scam, but although Mr A didn't intend his money to go to scammers, he did authorise the disputed payments. Lloyds is expected to process payments and withdrawals that a customer authorises it to make, but where the customer has been the victim of a scam, it may sometimes be fair and reasonable for the bank to reimburse them even though they authorised the payment.

### *Prevention*

I've thought about whether Lloyds could have done more to prevent the scam from occurring altogether. Buying cryptocurrency is a legitimate activity and from the evidence I've seen, the payments were made to a genuine cryptocurrency exchange company. However, Lloyds ought to fairly and reasonably be alert to fraud and scams and these payments were part of a wider scam, so I need to consider whether it ought to have intervened to warn Mr A when he tried to make the payments. If there are unusual or suspicious payments on an account, I'd expect Lloyds to intervene with a view to protecting Mr A from financial harm due to fraud.

The payments didn't flag as suspicious on Lloyds's systems. I've considered the nature of the payments in the context of whether they were unusual or uncharacteristic of how he normally ran his account, and I think they were. Both payments were to a legitimate cryptocurrency exchange, but they were high value payments to a high-risk cryptocurrency merchant and so I agree that Lloyds, ought to have intervened when he made the first payment.

I think a proportionate response would have been for Lloyds to have contacted Mr A and to have asked him some probing questions about the payment including why he was making the payment, whether there was a third party involved and if so how he'd met them, whether he'd downloaded remote access software, whether he'd been promised unrealistic returns, whether he'd made any withdrawals, whether he'd been coached to lie, whether he'd done any due diligence and whether he'd been advised to make an onwards payment from the cryptocurrency exchange.

But I don't think this would have uncovered the scam because Mr A's responses to the questions he was asked by his other banks tell me he wouldn't have disclosed key facts about the circumstances of the payments which would have led Lloyds to uncover the scam. He told R that he was paying a friend back for something they'd purchased on his behalf, and he told Bank T that he was moving funds to purchase a product. He also misled Bank N, and he told Bank H that there were no third parties involved and that he hadn't been told to lie.

Mr A's representative has argued that even if Mr A didn't disclose information to suggest he was the victim of a job scam, Lloyds should have warned him about job scams because they are so common. But I don't think it's reasonable to expect banks to give warnings about scam types that they don't reasonably suspect are happening. And I don't think a warning about job scams would have made any difference because made further payments to the scam after having received warnings from his other banks and he clearly trusted that the job was genuine to the extent that he was prepared to mislead his banks in order for the payments to be processed.

So, while I agree that Lloyds should have intervened, I don't think this represented a missed opportunity for it to have prevented the scam.

### *Recovery*

I've thought about whether Lloyds could have done more to recover the card payments when he reported the scam to it. Chargeback is a voluntary scheme run by Visa whereby it will ultimately arbitrate on a dispute between the merchant and customer if it cannot be resolved between them after two 'presentments'. Such arbitration is subject to the rules of the scheme — so there are limited grounds on which a chargeback can succeed. Our role in such cases is not to second-guess Visa's arbitration decision or scheme rules, but to determine whether the regulated card issuer (i.e. Lloyds) acted fairly and reasonably when presenting (or choosing not to present) a chargeback on behalf of its cardholder (Mr A).

Mr A's own testimony supports that he used cryptocurrency exchange to facilitate the transfers. It's only possible to make a chargeback claim to the merchant that received the disputed payments. It's most likely that the cryptocurrency exchanges would have been able to evidence they'd done what was asked of them. That is, in exchange for Mr A's payments, they converted and sent an amount of cryptocurrency to the wallet address provided. So, any chargeback was destined fail, therefore I'm satisfied that Lloyds's decision not to raise a chargeback request the cryptocurrency exchange company was fair.

And I don't think there was a realistic prospect of a successful recovery because Mr A paid an account in his own name and moved the funds onwards from there.

### *Compensation*

The main cause for the upset was the scammer who persuaded Mr A to part with his funds. I haven't found any errors or delays to Lloyds's investigation, so I don't think he is entitled to any compensation.

I'm sorry to hear Mr A has lost money and the effect this has had on him. But for the reasons I've explained, I don't think Lloyds is to blame for this and so I can't fairly tell it to do anything further to resolve this complaint.

### **My final decision**

For the reasons I've outlined above, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr A to accept or reject my decision before 12 September 2025.

Carolyn Bonnell  
**Ombudsman**