

The complaint

Mr and Mrs W complain that Lloyds Bank PLC (“Lloyds”) won’t refund them the money they lost when they fell victim to a visa scam.

As the payments now in question here were made from Mr W’s sole account, I will, for ease, refer to him throughout.

What happened

The background to this complaint is well-known to both parties, so I won’t repeat everything in detail again here. However, in summary, Mr W fell victim to a visa scam. He was tricked into sending multiple payments to someone who said they could obtain a “Certificate of Sponsorship” visa for his wife. Mr W was introduced to this person, who we now know to be a scammer, by an acquaintance who he believed had used his services before.

As part of the scam, Mr W made the following payments:

Date	Time	Amount
27/02/24	11:08	£4,000 (later refunded by scammer)
27/02/24	11:11	£1,000 (later refunded by scammer)
05/03/2024	07:50	£3,000
05/03/2024	10:24	£2,000
08/03/2024	17:06	£3,000
08/03/2024	17:17	£1,280
09/03/2024	09:41	£1,702
	Total Loss	£10,982

Mr W realised he’d been scammed when his wife didn’t receive the job offer / visa he had paid for and the scammer stopped communicating with him. So he raised the matter with his bank, Lloyds. Lloyds didn’t uphold Mr W’s complaint. It said there wasn’t anything that it could’ve done to protect him from falling victim to the scam.

Unhappy with Lloyds’ response, Mr W brought his complaint to this service where one of our investigators looked into things.

Our investigator didn’t uphold the complaint. They said it was reasonable for Lloyds’ to have declined to offer Mr W a refund. Mr W didn’t agree and as an agreement couldn’t 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.

In deciding what's fair and reasonable, I'm required to take into account relevant: law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to be good industry practice at the time.

Having done so, I've reached the same outcome as our investigator, for the same reasons and I won't be upholding his complaint. I'll explain why in more detail below.

Firstly, it's important for me to set out that I have been provided with little evidence to support this complaint. Mr W has provided his testimony as to what happened and a small number of screenshots of messages shared between him and the scammer – none of the screenshots provided show the scammer requesting the above payments or providing their account details. This means I have no evidence to connect the payments that left Mr W's account to the scam in question. Regardless, I have gone on to think about whether Lloyds has treated Mr W fairly when dealing with his complaint.

The first two payments that left Mr W's account were refunded to Mr W soon after they were made. As Mr W didn't suffer a loss in relation to these payments, I don't intend to comment on them further as part of this decision.

Lloyds' obligations:

To begin with, Lloyds has a primary obligation to carry out the payment instructions its customers give it. A customer will therefore be assumed to be liable for payments they have instructed to be made.

There is no dispute that Mr W authorised these payments, albeit having been deceived into believing he was sending them for the purpose of obtaining a visa and securing a job for a family member. On the face of it, he is therefore liable for the resultant losses. However, of particular relevance here, is the Lending Standards Boards Contingent Reimbursement Model Code ("the CRM Code").

The CRM Code says that the victim of an APP scam such as this should be reimbursed unless the bank is able to establish that one (or more) of the exceptions to reimbursement can be applied. Under the CRM Code, a bank may choose not to reimburse a customer if it can establish that*:

- The customer ignored what the CRM Code refers to as an "Effective Warning" by failing to take appropriate action in response to such an effective warning
- The customer made payments without having a reasonable basis for believing that:
 - the payee was the person the Customer was expecting to pay;
 - the payment was for genuine goods or services;
 - and/or the person or business with whom they transacted was legitimate

*Further exceptions outlined in the CRM Code do not apply to this case.

I think Lloyds has been able to establish that it may choose not to reimburse Mr W under the terms of the CRM Code. I'm persuaded one of the listed exceptions to reimbursement under the provisions of the CRM Code applies.

Did Mr W have a reasonable basis of belief?

I've thought about what Mr W has told us happened and based on the limited evidence provided to me, I'm not satisfied Mr W did have a reasonable basis for believing that the person he was transacting with was legitimate. I think there were a number of concerning factors here that ought to have made Mr W cautious and led him to complete more extensive research before making the payments he did. I say this because:

- It doesn't appear that Mr W has carried out any research to confirm the firm/or individual he was dealing with was either qualified or regulated to provide the services they were offering.
- While I understand Mr W has said he was dealing with an individual. When considering the formal nature of the service being paid for, the receipt of visa sponsorship and employment, I think it is questionable as to why he was paying accounts held by an individual, rather than to a firm that was clearly identifiable as offering these services.
- From the evidence I've seen, Mr W doesn't appear to have been provided with, nor asked for, any documentation from the fraudster, regarding the individual he was dealing with, nor regarding the actual job/visa he was making the payments for. Given the official nature of the service being provided, I think it would have been reasonable to have expected such documentation to be forthcoming.
- Alongside this, I don't think a legitimate individual or firm would ask for large sums of money upfront.
- I don't think it is typical for a legitimate firm/individual, particularly given the formal nature of the service requested here, to communicate through an informal messaging service.
- I haven't seen any evidence that supports that Mr W's acquaintance recommended this individual or that they or someone else had been able to successfully use their services in the past.

I can understand how in isolation any one of these things may not have prevented Mr W from proceeding. But when taken collectively, I think there was enough going on here that Mr W ought to have acted far more cautiously than he did and should have had significant concerns about the transactions he was making.

Overall, I find that Mr W ought to have done more to verify that the person he was dealing with was actually able to offer the services they were promising.

Effective warnings

I've gone on to think about whether Lloyds did what was expected of it at the time Mr W made the payments. Good industry practice requires that regulated firms such as Lloyds engage in the monitoring of customer accounts and be on the lookout for suspicious or out of character transactions with an aim of preventing fraud and protecting customers from financial harm. And under the CRM Code, where it identifies a risk of a customer falling victim to an APP scam, it is required to provide that customer with an "effective warning".

We now know, with the benefit of hindsight, that Mr W was falling victim to a scam. But based on the information that was available to it at the time, I don't consider Lloyds would've had any reasonable basis for believing that Mr W was falling victim to an APP scam at the time the scam payments were made. The payments ranged from £1,200 to £3,000 and Mr W often made payments similar to this from his account. He also had a history of making multiple payments in a single day. So, on balance, I don't consider the payments would have appeared as unusual or suspicious when compared to Mr W's usual account activity. With this in mind, when considering the CRM Code, Lloyds wasn't required to provide its

customer with an 'effective warning' – as defined in the CRM Code. So overall, I can't fairly or reasonably conclude that Lloyds hasn't met its obligations under the CRM Code now.

Vulnerability under the CRM code

Mr W has referenced the CRM Code's provision for vulnerable consumers. The CRM Code says that there are provisions under the Code which might lead to a refund, even when a customer doesn't have a reasonable basis for belief. The relevant part of the Code says:

"A Customer is vulnerable to APP scams if it would not be reasonable to expect that Customer to have protected themselves, at the time of becoming victim of an APP scam, against that particular APP scam, to the extent of the impact they suffered."

So, I've considered whether there were vulnerabilities present at the time to such an extent that Mr W was unable to take steps to identify the scam he fell victim to or to recognise steps he might take to test the legitimacy of what he was being told by the fraudster. To do so I must consider the details of the scam, Mr W's actions throughout, and the wider circumstances of what was happening.

Having thought about this carefully, on balance I think there is evidence within the circumstances that suggests Mr W was capable of taking steps to protect himself from fraud and financial harm. That is to say there was more he might reasonably have done that would have led to the scam being uncovered.

Mr W says that his mother was unwell at the time and he was hoping to sort out his wife's visa so he could travel to see her. Whilst I sympathise with Mr W's circumstances and understood why he was so keen to have his wife's employment situation finalised; I haven't seen any evidence from Mr W that persuades me that this meant that Mr W was unable to protect himself from the scam as set out in the CRM Code. I've not seen any evidence to suggest that it would be unreasonable to have expected Mr W to have carried out some research of checks on the person he was sending money to and in doing so protected himself from the particular scam he fell victim to. I've not seen any evidence to suggest Mr W didn't have the capacity and understanding to query the legitimacy of what was being offered.

Recovery

Finally, I have considered whether Lloyds did all it could to try and recover the money Mr W lost. It wasn't until several months after the payments were made that Mr W raised this matter with Lloyds. So, it was unlikely that there would have been a realistic prospect of success with any recovery attempt. Sadly, it is common for fraudsters to withdraw or move the money on as quickly as possible.

Summary

Overall, I don't find that Lloyds is liable to refund Mr W under the terms of the CRM Code. In saying this, I want to stress that I am very sorry to hear about what happened to Mr W and I am sorry he has lost out here. He was the victim of a cruel scam designed to defraud him of his money and I appreciate that he's out of pocket because of what happened. But I can only look at what Lloyds was and is required to do and I'm not persuaded that Lloyds is required to refund him under the CRM Code, nor that it was at fault in making the payments Mr W had instructed it to make or for any other reason.

My final decision

My final decision is that I don't uphold this complaint against Lloyds Bank PLC.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W and Mrs W to accept or reject my decision before 26 January 2026.

Emly Hanley Hayes
Ombudsman