

The complaint

Miss E complains that Lloyds Bank PLC won't reimburse the money she's lost to a scam.

What's happened?

Miss E says she's fallen victim to a romance scam. She paid the scammer £12,430 over eight transactions instructed between 8 July and 17 August 2021 to the same beneficiary. The transactions amounts are set out in the table below.

Date of payment	Amount of payment
8 July 2021	£1,000
16 July 2021	£600
19 July 2021	£690
26 July 2021	£2,440
29 July 2021	£2,260
3 August 2021	£1,970
6 August 2021	£2,380
17 August 2021	£1,090

Miss E has explained that:

- She met the scammer on a popular dating app in February 2021. She primarily communicated with him via text message, but she isn't able to provide any of those messages now.
- The scammer asked her to pay money into his friend's account, due to restrictions on his own account. The first time he asked her for money, it was to enable him to place a football bet. Then he began asking her for money to buy tools and safety equipment to help him tackle Turkish wildfires.
- She had no reason to think she was being scammed. She'd been friends with the scammer for a long time before he began asking her for money, and the reasons he gave for needing money made sense.

Lloyds intervened on 30 August 2021 when Miss E attempted to send a further £4,000 to the scammer via a new receiving account, and the scam was brought to a halt.

Miss E would like Lloyds to reimburse her financial loss under the provisions of the Lending Standards Board's Contingent Reimbursement Model ('CRM Code'). She says that:

- Her divorce was finalised shortly after she met the scammer. It was a traumatic time for her, and she was vulnerable to anyone seeking to make new connections with her.
- The disputed transactions were out of character and Lloyds should've intervened to prevent the scam.

Lloyds declined to reimburse Miss E under the CRM Code, and it was unable to recover any of her funds from the receiving account.

What did our investigator say?

Our investigator recommended that Lloyds reimburse 50% of Miss E's financial loss. She didn't think that Lloyds had provided Miss E with an effective warning/s to protect her from the scam, but she didn't think that Miss E had a reasonable basis for belief in making the payments either.

Miss E didn't accept our investigator's recommendation. She said that:

- By the time she sent the scammer money, she had been speaking to him for a long time – she didn't just send money to a person she didn't know.
- She believed the scammer when he said he was having issues with his bank account, so she needed to send him money via his friend.
- The disputed transactions were out of character.
- She stopped making payments to the scammer as soon as Lloyds intervened, and she wouldn't have lost any money to the scam if Lloyds had intervened sooner.

Miss E's complaint has now been passed to me to decide.

My provisional decision

I issued my provisional decision on 13 September 2023. I'll set out my findings below.

Lloyds has signed up to the CRM Code, and it was in force when the scam payments were made.

In summary, the CRM Code says that a customer who was vulnerable when they made an Authorised Push Payment ('APP') as part of a scam should receive a full refund of that payment, regardless of whether the firm knew about the customer's vulnerability before the scam took place. The CRM Code states that:

"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."

Miss E has said that her divorce finalised shortly after she met the scammer, and before she made the scam payments. It was a traumatic time for her – she was stressed, and her mental state was poor – and she was vulnerable to anyone seeking to make new connections with her. Miss E has my sympathies. I don't doubt that she was going through a difficult time. But I'm not persuaded that the circumstances she's described rendered her unable to protect herself from a romance scam, or that she can't reasonably have been expected to protect herself from the scam because of her vulnerability.

Nevertheless, the CRM Code requires firms to reimburse customers who have been the victims of APP scams, like the one Miss E has fallen victim to, in all but a limited number of circumstances. Lloyds has argued that one of the exceptions applies in this case. It says that Miss E made the payments without a reasonable basis for belief that the payee was the person she was expecting to pay, the payments were for genuine goods or services and/or the business or person she was transacting with was legitimate.

In thinking about whether Miss E had a reasonable basis for belief, I've considered what steps she took to reassure herself about the legitimacy of the transactions, and whether it was reasonable for her to proceed with the payments.

I've noted that Miss E did not meet the scammer in person, and she's said that her attempt to have video communication with the scammer was unsuccessful. She has not been able to provide any evidence that she built up a relationship with the scammer over several months before he began asking her for money as she's said or provide copies of any communication she had with the scammer. So, I can't reasonably conclude that it was reasonable for her to proceed with the payments on the basis of a trusting relationship built up over time with a known individual.

In addition, considering Miss E's testimony, I think there were some red flags she ought to have picked up on. For example, I think it ought to have caused her some concern that the scammer's account was apparently continuously blocked, so she needed to pass payments to him through his friend's account. If the account was continuously blocked as the scammer claimed, I would question how he was receiving Miss E's money from his friend and using it to fund the goods and services it was intended for.

The payment amounts were not insignificant considering the stated purpose - £1,000 for a football bet and £11,430 to buy tools and safety equipment. I don't consider that the story the scammer gave Miss E about needing to buy his own tools and safety equipment at a cost of £11,430 to battle Turkish wildfires was plausible, even considering Miss E's testimony that the media was reporting on the incident at the time. I have to question why Miss E didn't test the scammer's story before agreeing to send him large amounts of money, or question why he needed to place the relevant bet.

Overall, I don't think I can reasonably conclude that Miss E had a reasonable basis for belief on this occasion. So, I'm not persuaded that Lloyds should have reimbursed Miss E's loss because of any obligation under the CRM Code.

I've seen the warning that Lloyds gave Miss E when she instructed the first scam payment, and I think it could've been better. But I wouldn't have expected the bank to have identified an APP scam risk with any of the scam payments, so it wasn't required to provide Miss E with an effective warning under the CRM Code.

I appreciate that the scam payments were some of the highest value payments out of Miss E's account in the months leading up to the scam, and they went to a new payee. But I don't think they should have stood out to Lloyds as particularly unusual or suspicious. I wouldn't consider any of the scam payments to be high value enough for them to have caused the bank some concern on that basis alone. In June 2021, Miss E made a genuine faster payment for £1,135. The payment went to a known payee, but it was higher in value than the first scam payment – and it isn't unusual for account holders to transact with new payees on occasion. By the time the scam payments began to increase in value on 26 July 2021, Miss E was transacting with a known payee she'd developed a pattern of making regular payments to. None of the scam payments drained Miss E's account, and they weren't made in quick succession as might be expected in cases of fraud. It wasn't unusual for Miss E to fund outgoing payments by moving savings into her account.

Overall, I'm satisfied that Lloyds was entitled to consider there was no apparent APP scam risk here. So, I'm not persuaded that the bank needed to provide Miss E with an effective warning/s and I don't think it ought to make a difference to the outcome of this case that the warning Lloyds did provide fell short of being an 'effective warning'.

I haven't identified any other reason why Lloyds ought to have contacted Miss E about the scam payments she instructed before processing them. So, I'm not persuaded that Lloyds needs to reimburse Miss E's financial loss.

Finally, I've seen evidence which satisfies me that none of Miss E's funds remained in the beneficiary account for recovery by the time she reported the scam to Lloyds.

Responses to my provisional decision

Lloyds didn't respond to my provisional decision.

In summary, and in relation to her vulnerability and basis for belief, Miss E said:

- The difficult circumstances she was going through at the time made her vulnerable to a romance scam, and this should at least be taken into account when considering her reasonable basis for belief.
- She met the scammer on one occasion and had a few video calls with him.
- It isn't fair to take her inability to provide copies of any communication she had with the scammer into account because the messages they exchanged were automatically deleted when she reported and blocked him as she was advised to do. There is no reason to doubt her recollection of events and she has been very forthcoming with information when requested.

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 remain satisfied that it would not be fair or reasonable for me to instruct Lloyds to reimburse Miss E's financial loss.

I would like to assure Miss E that I took her circumstances into account when reaching my provisional decision. She hasn't provided any new information in relation to her circumstances at the time she was scammed that I haven't already considered. I'm still not persuaded that she can't reasonably have been expected to protect herself from the scam and, although I accept that she may have been unusually open to anyone seeking to make new connections with her, I'm still not persuaded that it would be reasonable to conclude that she had a reasonable basis for belief on this occasion for all the reasons I have already set out.

As I explained in my provisional decision, I have not seen any evidence in support of Miss E's testimony that she built up a relationship with the scammer over several months before he began asking her for money. Similarly, I have not been provided with any supporting evidence that she met the scammer in person or had successful video calls with him. But my findings in relation to Miss E's basis for belief do not turn on this. In thinking about whether Miss E had a reasonable basis for belief, I've considered what steps she took to reassure herself about the legitimacy of the transactions, and whether it was reasonable for her to proceed with the payments. In summary:

- I think there were red flags that Miss E ought to have picked up on – such as the scammer's account being apparently continuously blocked.
- I don't think the story the scammer gave Miss E about needing £1,000 to place a football bet and £11,430 to buy his own tools and safety equipment to battle Turkish wildfires was plausible.
- Miss E doesn't appear to have tested the scammer's story before agreeing to send him large amounts of money.

My final decision

For the reasons I've explained, I've decided not to uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss E to accept or reject my decision before 17 November 2023.

Kyley Hanson
Ombudsman