

The complaint

Mr R is unhappy that Lloyds Bank PLC ("Lloyds") won't refund him the £6,500 he lost when he fell victim to a vehicle purchase scam.

What happened

The circumstances that led to this complaint are well known to both parties, so I won't repeat them in detail here. But, in summary:

In October 2021, Mr R saw a private advert for a vehicle on a well-known online marketplace. He contacted the seller and agreed a price which included delivery. On 30 October 2021, Mr R transferred £6,500 to the business he thought he'd purchased the vehicle through. However, when the vehicle wasn't delivered and he couldn't contact the seller anymore, he realised he'd been scammed.

The bank said it didn't believe the payment Mr R made was unusual considering his normal account activity or that it should have flagged for further fraud/security checks. It also felt that Mr R didn't carry out sufficient verification checks to provide him with a reasonable basis for believing the seller genuinely owned the vehicle and that it was for sale.

Our investigator did not uphold the complaint as she felt that Mr R didn't have a reasonable basis for belief and that a warning wouldn't have made a difference.

Mr R's representative accepted the investigator's conclusions regarding Mr R's reasonable basis for belief. But it felt that the payment purpose along with paying a business account as a new payee ought to have raised concerns with the bank. It therefore felt a 50% refund was appropriate.

I wrote to Mr R's representative informally as I was minded to reach the same overall conclusion as the investigator but wanted to expand on the reasoning given.

In particular I explained that Mr R's payment purpose choice made it very difficult for Lloyds to give a tailored and impactful warning. So, I didn't find that Lloyds had failed in its obligation to provide an effective warning. But I also concluded that as Mr R didn't see the relevant warning - I couldn't say Mr R ignored an effective warning either. I also explained why I didn't consider Lloyds could have done more to try and prevent the scam or recover Mr R's funds once it knew he'd been the victim of a scam.

Mr R disagreed. Mr R does not agree that a warning was provided to him and would like a copy of the warning to be given. He also wishes to make it clear that he did not select the incorrect payment purpose intentionally and believes this was the most suitable option at the time.

As the case could not be resolved informally, I need to reach a final decision in this case.

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; regulatory rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the time.

In broad terms, the starting position at law is that a firm is expected to process payments and withdrawals that a customer authorises, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. There's no dispute here that Mr R authorised the payment.

However, where a customer makes a payment as a consequence of the actions of a fraudster, it may sometimes be fair and reasonable for the bank to reimburse the customer even though they authorised the payment. When thinking about what is fair and reasonable in this case, I've considered whether Lloyds should have reimbursed Mr R in line with the provisions of the CRM Code it has agreed to adhere to and whether it ought to have done more to protect Mr R from the possibility of financial harm from fraud.

There's no dispute here that Mr R was tricked into making the payment. He thought he would receive a vehicle in exchange for his money and this wasn't the case. But this isn't enough, in itself, for Mr R to receive a refund of the money under the CRM Code.

The CRM Code

Lloyds has signed up to the Lending Standards Board Contingent Reimbursement Model (the CRM Code). The CRM Code requires firms to reimburse customers who have been the victims of Authorised Push Payment (APP) scams like this, in all but a limited number of circumstances.

It is for Lloyds to establish that one or more of the exceptions apply as set out under the CRM Code. Those exceptions are:

- Mr R ignored an "effective warning" in relation to the payment being made.
- Mr R made the payment without a reasonable basis for believing that: the payee was the person he was expecting to pay; the payment was for genuine goods or services; and/or the person or business with whom Mr R transacted was legitimate.

There are further exceptions within the CRM Code, but they do not apply in this case.

The CRM Code also outlines the standards a firm is expected to meet. And it says that when assessing whether the firm has met those standards, consideration must be given to whether compliance with those standards would have had a material effect on preventing the APP scam that took place.

Having considered everything, while I'm sorry that Mr R has been the victim of a cruel scam, I agree with the outcome reached by the investigator broadly for the same reasons.

As Mr R's representative has accepted the investigator's conclusions about reasonable basis of belief - I've haven't gone over those details again – but I do agree with those conclusions. Instead, I have focused on the reason Mr R and his representative asked for a decision.

Did Lloyds meet its obligations under the CRM Code and did Mr R ignore an effective warning?

The CRM Code says that effective warnings should be risk based and, where possible, tailored to the APP scam risk indicators and any specific APP scam types identified through the user interface with which the customer is initiating the payment instructions.

It seems that Lloyds did provide a warning for “moving my money” which is what Mr R selected at the time the payment was processed. I haven't repeated the warning that was shown during the online payment process because Mr R's choice made it very difficult for Lloyds to give a tailored and impactful warning. It's also the case that, had answering as he arguably ought to have done (by selecting “something bought online”) led to a warning that met the definition of “effective” under the CRM Code (that's not a finding I need to make here), it would be irrelevant because Mr R didn't see that particular warning. So, I don't find that Lloyds has failed in its obligation to provide an effective warning, but I can't say Mr R ignored an effective warning either.

I appreciate Mr R did not intentionally select the incorrect payment purpose. But it would still not be fair for me to conclude Lloyds failed in its obligation to provide an effective warning on this basis. Neither would it be fair for me to conclude Mr R ignored an effective warning – that's because he didn't see the most appropriate warning.

Mr R acknowledged he selected an alternative payment purpose – indeed this formed part of his representative's detailed submissions about the fact this ought to have flagged as a concern with Lloyds. So, the warning that triggered wasn't relevant to his circumstances and for the reasons I've explained above – that warning is not material to this decision. I appreciate Mr R would like to see a copy of the warning and evidence of it, but I have already said this is not relevant or material to my decision in this case. So, I don't think providing this to Mr R makes a difference to my outcome.

Mr R's representative also originally complained that Mr R didn't see a “purchasing something online” warning – thereby acknowledging this was the most appropriate option.

I appreciate Mr R says he didn't see a warning but it's more likely than not an automatic warning would have popped up in response to the payment purpose given. Although I do appreciate Mr R might now not recall seeing it.

Should Lloyds have done more to try and prevent the scam and protect Mr R?

As well as the CRM Code, a bank still has wider obligations and a duty to protect its customers, as far as is reasonably possible, against the risk of financial harm from fraud and scams. As such, there are circumstances where it might be appropriate for a bank to take additional steps or make additional checks before processing a payment to help protect its customers from the possibility of financial harm from fraud.

Mr R's representative argues that the payment purpose “move my money” along with then paying a business account as a new payee ought to have raised concerns. It has argued that the paying of a business account does not match the payment purpose and the bank should have consequently made contact with Mr R and the scam would have unravelled. I understand the argument it is making but I don't think Lloyds would have had reason to be concerned. Overall, the payment doesn't look unusual or suspicious. Mr R had made a number of faster payments for high value amounts over the months prior to the scam. He had also made several large transactions that appear to be vehicle related. Banks can't reasonably be involved in every transaction. There is a balance to be struck between identifying payments that could potentially be fraudulent and minimising disruption to legitimate payments. I am mindful that the payment purpose selected is quite general and

could be open to interpretation. I think it unrealistic to expect a bank to be involved every time a consumer enters a payment journey that *might not* match the assumed purpose of the destination account. It did appear to be going to a business account rather than an individual - arguably adding to an element of legitimacy. Overall, I don't think the transaction Mr R made stood out as being unusual based on his historical activity or that Lloyds ought reasonably to have identified a risk based on the consumer's payment purpose entry and the type of account or name on the destination account.

Did Lloyds do enough to recover Mr R's funds?

I've thought about whether Lloyds took reasonable steps to recover Mr R's funds once it was made aware he was the victim of a scam. The scam payment was made on 30 October 2021 at 18:42 and Mr R reported the scam to Lloyds on 1 November 2021. Lloyds contacted the receiving bank the same day but no funds remained. I have seen the evidence which shows all the money had left the scammers account by 19:10 on 30 October 2021. So before Mr R had a chance to report it to Lloyds. This is not unusual as scammers usually remove funds within hours. So Lloyds couldn't have done any more to try and recover Mr R's money.

I realise my decision will be a significant disappointment to Mr R. I sympathise with his circumstances, and I am sorry he has fallen victim to a scam. But having considered all the evidence and arguments, I'm not upholding his complaint.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr R to accept or reject my decision before 19 October 2023.

Kathryn Milne
Ombudsman