DRN-3709672

## The complaint

Mr T is unhappy that Lloyds Bank PLC won't refund the money he's lost to a fraudster.

## What's happened?

Mr T has fallen victim to a safe account scam. He says that, on 15 July 2021, he received a call from Lloyds' fraud team – the incoming call came from the same telephone number as the one on the back of his bank card. The caller knew his name and address, and they had access to details about his bank account. The caller told him that two fraudulent transactions had been attempted on his account. They asked him to login to online banking and, when he did, he saw that someone had also moved some money from his savings account to his current account. The caller told him that his accounts were at risk and he needed to move his money to a 'safe account' to protect it – he would receive a bank card for the new account within a few days.

Mr T says he was talking to the caller for approximately two hours. During that time, he was instructed to transfer £5,000 from his current account to his partner's account ('the payment'). The caller then got in touch with his partner and instructed her to move the money from her bank account to the 'safe account'. They said they would move the remaining money in Mr T's accounts to the 'safe account', but this never happened.

Mr T realised later that he'd been scammed and reported the matter to Lloyds. Lloyds declined to reimburse him on the basis that he hadn't suffered a monetary loss as he'd transferred his funds to his partner's account, and it was her that lost the funds when she transferred them from her account to the scammer's.

What did our investigator say?

Our investigator found that Lloyds should have reimbursed Mr T under the provisions of the Lending Standards Board's ('LSB') Contingent Reimbursement Model ('CRM Code'). Lloyds didn't agree. The bank maintained that Mr T hasn't suffered a monetary loss and it:

- said that it wasn't required to intervene with the payment because it followed a credit which made it appear likely that it was an intended payment, and it went to a known payee, so it wasn't suspicious.

- intimated that Mr T didn't have a reasonable basis for belief when he made the payment.

Mr T's complaint has now been passed to me to decide.

## 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.

Lloyds is a signatory of the CRM Code, which requires firms to reimburse customers who

have been the victims of Authorised Push Payment ('APP') scams, like the one Mr T has fallen victim to, in all but a limited number of circumstances.

I note that Lloyds has argued Mr T hasn't suffered a monetary loss in this case, but I can't agree. The funds that were ultimately lost to the scammer belonged to him – they just passed through his partner's account on the way to the scammer. Fraudster's use this tactic to make it harder for banks to identify a scam risk, and to make it more difficult for banks to trace and recover their victim's funds. I think that Lloyds, with its industry knowledge of fraud, ought to be aware of this. In any event, the LSB has confirmed that the CRM Code includes cases, such as this one, where a victim was tricked into sending money to a scammer's account via a family member or friend's account and the funds are now lost. So, I'm satisfied that Mr T's complaint falls within the scope of the CRM Code.

Lloyds has acknowledged that it didn't provide Mr T with an effective warning during the payment journey. It says it wasn't required to do so. And the bank's intimated that Mr T made the payment without a reasonable basis for belief 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 he was transacting with was legitimate.

Effective warning

The CRM Code requires a firm, where it identifies an APP scam risk in the payment journey, to take reasonable steps to provide the customer with effective warnings. This should include appropriate actions for customers to protect themselves from APP scams. The CRM Code requires firms to consider payments instructed against normal transactional data and customer behaviour.

I appreciate what the bank has said about the payment going to a known payee. But I don't consider the provision of an effective warning to be as onerous as blocking a payment or contacting a customer directly, so I think the threshold should typically be lower than I might expect a non-CRM Code APP scam trigger to be. I've looked at Mr T's account statements and I can see that, although the payment went to a known payee, it was the highest value transaction on his account by far in the preceding six months – Mr T typically made very low value transactions. And it immediately followed a large transfer into the account from Mr T's savings account, which can point to fraudulent activity. So, I think there was enough going on here to expect Lloyds to have provided Mr T with an effective warning, despite the payment destination. The bank acknowledges that it didn't provide Mr T with an effective warning, so I'm not persuaded that it can rely on this exception to reimbursement.

Reasonable basis for belief

Overall, I'm satisfied that Mr T had a reasonable basis for belief in this case. I acknowledge that there were some 'red flags' in the scammer's story – for example, it's unclear why Mr T believed his funds needed to be moved on from his partner's account when it was his account that was at risk. But Lloyds didn't make the scam risk clear to him. And ultimately, in the heat of the moment, when he thought his funds were at risk, he was persuaded that the caller was genuine because:

- they called from a spoofed number, which matched the number on the back of his bank card.
- they knew some of his personal details, and details about his account.
- he saw that money had been moved from his savings account to his current account, which fit with the scammer's story.

Considering everything, the fraud was sophisticated, and I don't think it's unreasonable that it went undetected by Mr T, who was convinced that the caller was genuine in all of the circumstances.

Conclusions

To conclude, Lloyds should have reimbursed the money Mr T lost to this scam under the terms of the CRM Code. I'm satisfied that the payment is covered by the Code, and I'm not persuaded that any of the permitted exceptions to reimbursement apply. So, the bank should now reimburse Mr T's financial loss and pay interest at the savings account rate (because I consider it likely that Mr T's funds would have remained in the savings account, at least for the time being, if he had not been defrauded) from the date it should have reimbursed him under the CRM Code to the date of settlement.

**My final decision**

For the reasons I've explained, my final decision is that I uphold this complaint and instruct Lloyds Bank PLC to:

- reimburse Mr T's loss within 28 days of receiving notification of his acceptance of my final decision; plus

- pay interest at the savings account rate from the date Mr T should have been reimbursed under the CRM Code to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr T to accept or reject my decision before 26 October 2022.

Kyley Hanson
**Ombudsman**