DRN-5039620

The complaint

Mr A complained because Lloyds Bank PLC refused to refund him for payments which he said he didn't authorise.

What happened

At 12.24 pm on 6 June 2024, £5,000 was transferred from Mr A's Lloyds savings account to his current account. One minute later, there was the first of seven outgoing payments, made between 12.25 pm and 13.45pm. These were to a merchant Mr A had previously paid for genuine transactions. The total of the debits for the seven payments was £4,497.55.

Mr A rang Lloyds later the same day. He said he was on holiday abroad, and hadn't made the payments, or the £5,000 transfer. At this point, the payments were pending, but Lloyds explained that it couldn't cancel them while they were pending. Lloyds cancelled Mr A's internet banking at his request, and advised him to contact the merchant.

Mr A rang again the next day. Lloyds' fraud team asked Mr A some questions. Mr A said no-one had contacted him unexpectedly; he hadn't clicked on any unusual links; and hadn't given anyone his details. Mr A said he had two devices on which the Lloyds mobile banking app was installed, though he said he'd lost one of them. He said the mobile banking app wasn't working on the other one.

On 23 June, Mr A rang to chase his refund. Lloyds told him the claim had been declined, and Mr A complained.

Lloyds sent its final response to Mr A's complaint on 25 July. It said that as part of investigating a fraud claim, it considered the information Mr A had given, the activity on his account, and the information it held on its systems. It said that its records showed that at the time of the payments, Mr A had been logged in to his internet banking. He'd told Lloyds that no-one else had access to his internet banking, or knew his password. So there was no explanation for how a fraudster could have accessed Mr A's device and made the payments. Lloyds said that if Mr A still believed the payments were fraudulent, he could contact the merchant direct.

Mr A wasn't satisfied and contacted this service. He said that he'd lost his phone to a pickpocket on 25 May, when he'd been on holiday, but Lloyds had refused a refund because the transactions had been made on his phone.

Our investigator didn't uphold Mr A's complaint. She said that the evidence showed that a new device had been registered for online banking on 25 May, in addition to the existing device. On 4 June, there had been a password reset on the new phone, and biometrics had been updated. It had needed Mr A's security information to complete this. Lloyds had sent a text to Mr A's old phone confirming the changes.

The old device, on which the disputed transactions took place, had been accessed on 6 June at 12.12pm, with the password and memorable information correctly entered. The investigator pointed out that as Mr A had confirmed that he hadn't stored any of his online

banking security information on his phone, she couldn't see any point of compromise whereby a third party could have found out this information.

Mr A didn't agree. He said that all Lloyds had said was about the passcode and how fraudsters had obtained this. He said that was something that needed to be looked into, not just asking how anyone else would have known the passcode. Mr A said he thought the recipient merchant, or Lloyds staff, had been involved. He said we should question the recipient merchant.

Mr A also said he'd contacted Lloyds when the payments had still been pending and he was unhappy that Lloyds had said it couldn't stop them at that point.

Mr A asked for an ombudsman's 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.

First, it's accurate that pending payments can't be stopped. So this decision focuses on the disputed transactions, not on pending payments.

What the Regulations say

There are regulations which govern disputed transactions. The relevant regulations here are the Payment Services Regulations 2017. In general terms, the bank is liable if the customer didn't authorise the payments, and the customer is liable if they did authorise them. So what determines the outcome here is whether it's more likely than not that Mr A himself, or a third party fraudster, carried out the transactions.

The regulations also say that account holders can still be liable for unauthorised payments under certain circumstances – for example if they've failed to keep their details secure to such an extent that it can be termed ''*gross negligence.''*

Who is most likely to have authorised the disputed payments?

Mr A says that his phone was pickpocketed on 25 May. The disputed transactions took place on 6 June. I find it surprising that Mr A didn't report the theft to Lloyds until after the disputed transactions had taken place, several weeks later. It's also very surprising that any fraudster who obtained the phone on 25 May would have waited until 6 June before trying to profit from the theft.

I've looked carefully at the detailed technical evidence provided by Lloyds. This helpful evidence relates both to the transactions themselves, and to the history of the two phones.

If a third party had stolen Mr A's old phone, I can't see how that person could have known all the necessary security information which was needed in order to make the payments. Mr A told Lloyds that no-one else had access to his internet banking, or knew his password, and that he hadn't received any suspicious calls, or clicked on any suspect links. In Mr A's response to the investigator's view, he objected that Lloyds had focused on the passcode. But that is indeed the key relevant factor here – how would anyone else have known Mr A's secure details, including his passcode, memorable information, and other details, which were needed to make the payments?

I also note that Mr A had previously made payments to the same merchant. Looking through some of Mr A's bank statements, I see he made multiple undisputed payments to that merchant, for example in January, April and May 2024.

Mr A said that this service should contact the recipient merchant. But what determines the outcome is who authorised the transactions. The merchant which received the money couldn't know that, so its evidence couldn't address the main issue.

Mr A also suggested that Lloyds staff had been involved. I don't think this is at all likely. Whoever carried out the disputed payments had Mr A's phone in their physical possession. Mr A alleged that had been stolen when he was abroad. That person also knew Mr A's security information, which Mr A had set up himself, and biometric information to access the phone. That wouldn't have been accessible to one of Lloyds' staff.

Taking all these factors into account, I consider it's most likely that it was Mr A himself who carried out the transfer of money from his savings account to his current account, and the disputed payments. So Lloyds doesn't have to refund hm.

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 A to accept or reject my decision before 27 January 2025.

Belinda Knight
Ombudsman