DRN-4512468

The complaint

Mr B is unhappy that Lloyds Bank Plc won't reimburse him for a transfer made from his account which he says he didn't authorise.

What happened

On 15 August 2023, a payment of £500 was made from Mr B's account to a third party that he didn't recognise. He says he received a text message from Lloyds Bank confirming that a new payee had been set up. Mr B says he contacted Lloyds Bank immediately and informed them that he didn't recognise the payee, nor did he make the payment. He asked Lloyds Bank to refund him.

Lloyds Bank asked Mr B for his recollections of what happened on 29 July 2023 when a second device was registered. Mr B wasn't able to provide any recollections and he also couldn't remember receiving a security call. Mr B confirmed that no one else knew his online credentials such as password and memorable information. Lloyds Bank decided to decline Mr B's claim.

Unhappy with this, Mr B referred his complaint to our service. Our investigator said he was unable to identify how Mr B's online banking was compromised and the activity wasn't typical of fraud. On balance, he thought it was more likely than not that Mr B authorised the transaction.

Mr B disagreed and asked for an ombudsman's decision. He explained that he called Lloyds Bank to stop the transaction as soon as he was prompted by their text message. He says he had no idea who the payee was or why the payment was made. He feels this should clarify that he had no knowledge of this transaction. He feels that Lloyds Bank shouldn't have made the payment if they have the security messages in place which he acted upon.

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.

Under the relevant rules, Lloyds Bank can hold Mr B liable for the disputed transaction if the evidence suggests that it's more likely than not that he made or authorised it himself.

I've looked at the technical evidence provided by Lloyds Bank, and this shows that there were two registered devices on Mr B's account. One was Mr B's usual mobile device, which was registered on 19 October 2022. The second mobile device was registered a few weeks prior to the disputed transaction on 29 July 2023.

The audit reports show that access to Mr B's online banking to make the disputed transaction was correctly authenticated using biometrics on a second device registered on Mr B's account.

Mr B has told us that he only used his mobile device, and he never allowed a second device

to be added to his account. He also confirmed that no one had access to his mobile device, nor did he allow another device to be registered on his account.

I've had a look at the internet banking logs for 29 July 2023 – the date when the second device was added. The reports show that Mr B logged on using his mobile device at 3.52am and made a payment of £163 which isn't disputed.

I can also see that Mr B's mobile device continued to log on and off between making the payment at 3.52am until the second device was added. It also shows that Mr B's mobile device was logged on again a few minutes after the second device was registered.

I've looked at the steps a fraudster would've needed to follow in order to add the second device to Mr B's account. As a starting point, the fraudster would've required knowledge of Mr B's username, password and memorable information. He's told us that he hasn't written these down anywhere and hasn't shared them with anyone. So, it's difficult to understand how a fraudster obtained Mr B's online credential information.

The fraudster would've then required access to Mr B's mobile device which is the registered phone number on his account. This is because, as per the mobile banking registration process, Lloyds Bank would call the phone number registered on the account for a security check.

I can see from the internet banking log that Lloyds Bank called Mr B on his registered mobile number to confirm the four-digit security code which would've appeared on the second device. The correct code was confirmed and therefore the second device was registered on Mr B's account.

Mr B has told us that only he had access to his mobile device when the second device was registered, and he didn't allow a second device to be added. Based on this, there doesn't seem to be a plausible explanation for how a fraudster could've accessed Mr B's online credentials and his mobile device to register for mobile banking.

I can also see that the activity on the second device doesn't appear to be consistent with fraud. This is because the second device logged on at 1.02am on 15 August 2023 which was less than half hour after funds of £1,700 were credited into the account but logged off shortly after at 1.16am without making any transactions on the account.

I find it unlikely that a fraudster would decide to delay making transactions when funds had been credited into the account. Also, the fraudster logged on again at around 1.40am to only transfer out £500, leaving a significant balance in the account of around £1,200. It's more likely for a fraudster to drain the account of the available funds as quickly as possible to maximise gain before the account holder could discover the fraudulent activity and notify their bank to put a block on the account.

Even if I accept that Mr B's actions shortly after the disputed transaction suggests he wasn't aware of it, I'm afraid he can still be held liable for the transaction in this instance. I say this because, all the evidence points to Mr B authorising the second mobile device to be registered on to his account. And in doing so, he's effectively authorised the disputed transaction, even if he wasn't aware of, or agreed to it.

Although Mr B responded quickly to the text message, the disputed transaction left his account immediately, so it was too late to stop the transaction. But the second device was de-registered to prevent any further transactions being made.

All things considered, I think the most plausible explanation is that Mr B either made or

authorised the transaction by allowing another party access to his online banking, so I can't ask Lloyds Bank to reimburse him.

My final decision

For the reasons explained above, my final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 20 June 2024.

Ash Weedon
Ombudsman