DRN-4788558

The complaint

Mrs S complains that Lloyds Bank PLC ("Lloyds") held her responsible for transactions she didn't recognise.

What happened

Mrs S received a call from Lloyds about some payments leaving her account. Lloyds had noticed that some further checks to verify some of those payments weren't completed correctly. They discussed several transactions with Mrs S that she said she didn't recognise. These had taken place over several weeks, starting the previous month, totalling about £450 in disputed transactions.

Mrs S confirmed she still had her card and no one else had access to it, or her mobile phone. Some of the payments Mrs S didn't recognise required additional steps before they were completed. Lloyds confirmed that messages were sent to Mrs S registered mobile phone and the appropriate response was received to allow those payments to be completed. Additionally, Lloyds looked at some of the audit data concerning these transactions and confirmed the phone was used from a consistent location based on the IP address data.

Mrs S continued to deny any involvement in the disputed transactions and asked for a refund. Lloyds declined to pay this as they believed the evidence showed those transactions could only have been made by Mrs S.

Mrs S remained unhappy with her complaint and brought it to the Financial Ombudsman Service for an independent review where it was looked into by one of our investigators. Both parties were asked for evidence and Mrs S explained she hadn't been very well during the period that the disputed transactions had taken place, so hadn't paid a lot of attention to her credit card account. She said her phone was kept in a locked cupboard, and she would know if anyone else had used it. Mrs S confirmed she had access to her account through online banking but didn't use her phone to do this. Mrs S was also able to say no one else had access to her card or the card information and she hadn't given permission to anyone else to use it.

Lloyds confirmed the audit data showed a consistent IP address linked to both disputed transactions and undisputed transactions. They showed evidence of how the account was accessed, using Mrs S's phone and another device, including a payment made towards the balance of the credit card from the same IP address.

After reviewing the evidence, the investigator thought it reasonable for Lloyds to hold Mrs S responsible for the payments and didn't uphold her complaint. It was commented that Lloyds sent messages to Mrs S's registered phone and received positive responses before releasing some of the payments.

It was also accepted that whilst IP address data can be compromised, other evidence including audit data showing Mrs S's phone had been used to log into the account during the period the disputed transactions took place. So, it was reasonable to conclude that Mrs S made the payments herself.

Mrs S disagreed and asked for a further review of her complaint. She commented that fraudsters were capable of carrying out these payments and the type of payments were out of character for her usual spending.

As no agreement could be reached, the complaint has now been passed to me for a 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.

The relevant law surrounding authorisations are the Payment Service Regulations 2017 and the Consumer Credit Act 1974. The basic position is that Lloyds can hold Mrs S liable for the disputed payments if the evidence suggests that it's more likely than not that she made them or authorised them, but Lloyds cannot say that the use of the card details for online payments conclusively proves that they were authorised.

Unless Lloyds can show that consent has been given, it has no authority to make the payment or to debit Mrs S's account and any such transaction must be regarded as unauthorised. To start with, I've seen the bank's technical evidence for the disputed transactions. It shows that the transactions were authenticated using the payment tools issued to Mrs S.

It's not our role to say exactly what happened, but to decide whether Lloyds can reasonably hold Mrs S liable for these transactions or not. In doing so, I'll be considering what is most likely on a balance of probabilities.

It's the case here that Mrs S denies making any of the transactions she's disputed, whilst Lloyds believe she was responsible. Mrs S explained how she keeps her card secure, together with her phone and no one else has access to them. Mrs S hadn't visited any suspicious websites or been asked to click on any unusual links. On this basis it seems unlikely anyone could obtain the necessary details to make the payments.

Additionally, Mrs S's phone was sent several security messages requiring a response before certain transactions were finalised. Because Lloyds received them, the payments were made. Mrs S denied receiving those messages, but it seems unlikely the messages were somehow manipulated by a fraudster; more likely they were successfully sent to the phone Lloyds had registered on Mrs S's account.

Lloyds also had IP address data - which is a means to identify physical locations that online transactions/devices are connected to and can be their actual physical location or other locations connected to the provider of the data services.

What this means for the complaint is that Lloyds have shown that numerous transactions that haven't been disputed, and various uses of Mrs S's mobile banking were made from a consistent IP address as those recorded by some of the disputed transactions. Put simply that means the (phone) used to receive the messages/respond to the bank was in the same location when other undisputed transactions were made.

Whilst Mrs S has said she didn't use her phone for mobile banking, Lloyds evidence shows her phone and another device being used on several occasions throughout the period of the disputed transactions to log into her mobile banking account. So, on balance the evidence points to Mrs S's phone being used to answer certain security messages and monitor her account. Given that she herself has ruled out anyone else using her account, it seems unlikely that those transactions could have been carried out by anyone else without her knowledge. I don't think there's a plausible explanation that somehow an unauthorised third party was able to gain access to Mrs S's device(s), make these transactions and return the device without her being aware of it, particularly given the location information provided by the bank.

I did note that some of the payments were to businesses involved in "membership" packages. They appear to offer products in exchange for a fee and it's not unusual to see these types of payments linked to complaints. Often, a purchase is made which carries with

it a commitment to make payments for the “membership” and sometimes it’s not clear what has been signed up to.

I don’t know exactly what happened here and given Mrs S has denied making any payments to the merchants she’s disputed; I’ve had to make my decision based on the overall evidence. On balance, I think it’s implausible to conclude they weren’t authorised without stronger evidence to the contrary. That means I think it’s more likely than not that Mrs S carried out these transactions herself – or that someone else with consent did so.

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 Mrs S to accept or reject my decision before 26 September 2024.

David Perry
Ombudsman