

The complaint

Mr S complains about Lloyds Bank PLC's system. It asks him to verify his account when he tries to log on after travelling abroad and he thinks it's monitoring his movements.

What happened

Mr S regularly uses his Lloyds on-line account. So he doesn't have to rely on verification calls, he's entered 'trusted site' on his computer.

Mr S regularly travels abroad and every time he returns, he has no choice but to call Lloyds and await a security code. He finds this inconvenient and stressful.

As this only occurs when he returns from travelling abroad, he's mystified and concerned about how they know this private information.

Mr S has complained about this to Lloyds several times, but they say there is nothing they can do. They explain that they undertake Strong Customer Authentication (SCA) as they can *'see things like Location from IP addresses and this information is used for security and fraud prevention'*.

Mr S doesn't understand this as he doesn't take his computer away with him or use any device to log on to his Lloyds account while away.

Mr S brought his complaint to our service, but our investigator didn't uphold his complaint.

As Mr S remains dissatisfied, his complaint has been referred to me to look at.

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.

Having done so, I'm not upholding this complaint, and I'll explain why.

I should first say there are limitations to how our service can help here. I say this because we aren't the regulator of financial services, and we can't interrogate a business system or tell them to make modifications. Also, we can't interrogate the systems of other parties.

However, what we can do is consider each individual case and, where we think a business hasn't acted fairly and reasonably in the circumstances, decide what should be done to put right any financial or non-financial losses that a consumer has experienced. So, we can ask a business to pay a proportionate level of redress.

From reviewing the file, it's clear that Lloyds have responsibilities to protect customer accounts and adhere to regulations. Mr S understands and accepts this and that there will be times where it's necessary for him to use the SCA and go through the additional security checks to access his account.

Mr S's complaint is that Lloyds haven't been able to explain why SCA is initiated every time he returns from his travels and their response has caused him to suspect they have information on his movements.

I reviewed the dates Mr S had returned from his travels and compared this with the data Lloyds have on him logging on to access his account, and from my analysis, I'm satisfied Mr S hasn't been accessing his account from overseas.

I noted that when Mr S said Lloyds seem to know when he is at home and overseas, they said *'This is correct, we can see a location of where a customer is logging on from using an IP address. This information is used for fraud prevention and not to monitor your movements'*. But from looking at the data, I think Lloyds' comment was a general statement and not specific to Mr S.

Mr S says none of Lloyds' common SCA trigger reasons apply to him and that this would suggest a connection with him returning from his travels, however from the information available to me, I don't think Lloyds have information on his movements or this is the reason for the issue.

I pointed this out to Lloyds and, as Mr S needs to use SCA each time he returns to the UK, I asked them if they would be prepared to further investigate and they:

- Said they're *'unable to pinpoint the reason when a SCA call is required when customers log in using a previously trusted device'*
- Gave the following list of possible reasons SCA might be triggered:
 - *If they log in using a new/different device, they'll need to 'trust again'*
 - *If they update or install a new browser, they'll need to 'trust this device' again after additional authentication*
 - *If they use an incompatible browser when logging on to the internet/online banking they'll need to update their browser*
 - *If they use in-private browsing, this doesn't allow devices to be trusted, so no prompt is generated*
 - *If they delete their browser data such as cookies or cache, they'll need to trust their device again following each deletion*
 - *If they've declined 'trust this device' after viewing it, it won't be offered again for another seven days*
 - *If there's technical issues with SDID being generated, prompts won't be offered until the issues are resolved*
 - *If they log on for the first time with a device browser, they won't be presented with 'trust this device' until logging on again*
 - *If they've activated contact blockers they won't be presented with the option to 'trust this device' until removed*
 - *If they don't meet certain protection trust rules, they won't be presented with the option to 'trust this device'. This may be because:*
 - *They have no, or out of date, anti-virus software on their device, they'll need to update this*
 - *They share the device with other people or in a public location*
 - *Where the device may be deemed untrusted for example, listed as bad or blacklisted device*

From looking at this list, together with Mr S's submissions, including the pattern of the issue occurring when he returns from his travels and him not using his device whilst he's away, I think it likely that he will be dissatisfied with this response as he thinks these reasons don't apply to him. However, it isn't possible to dismiss some of them. So, the cause of the issue will probably continue to be a mystery with him still suspecting Lloyds have information on his movements.

As mentioned above, where a dispute involves systems, I'm unable to interrogate either the business or customer hardware and software to identify the root cause. Also, I can't either expect or instruct Lloyds to undertake root cause identification work, which I think would be very difficult and costly, in order to pinpoint the exact reason for the issue.

I appreciate this will probably mean Mr S's frustrations will continue when he returns from his travels but, based on my review of the file, I can't either say that Lloyds have done anything wrong or instruct them to do any more. So, I'm not upholding this complaint.

My final decision

My final decision is that I'm not upholding this complaint against Lloyds Bank PLC.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 14 April 2024.

Paul Douglas
Ombudsman