DRN-3228237

The complaint

Mr H complains that Lloyds Bank PLC has stopped him accessing his online banking.

What happened

Mr H is a pensioner who has been a customer of Lloyds Bank for many years. He has two accounts with Lloyds Bank – an account with a debit card and an account with a credit card. He also has a credit card with another bank, but he only uses that card once a year.

In December 2020 Mr H complained to Lloyds Bank saying that he couldn't access his accounts online as Lloyds Bank had made changes to its logging in process. The changes meant he needed a mobile phone or a landline to receive a one-time passcode or a computer that he could make a "trusted device". Mr H said he'd been using internet banking for many years and used internet cafes. He said that he was hard of hearing and technically challenged and that he wanted to carry on using the method of logging on that Lloyds Bank had in place before the changes had taken place. He was in France when he complained.

Lloyds Bank investigated Mr H's complaint and said that it had made changes to its processes in order to implement strong customer authentication. It said its customers had four options: namely, receiving a one-time passcode on a UK mobile, using its mobile banking app, receiving an automated call to any telephone number or using a "trusted device". Lloyds Bank accepted that two of these options wouldn't work for Mr H as he didn't have a UK mobile number or use its mobile app, that the second option wouldn't work as he didn't want to use the telephone and that the final option – using a "trusted device" – wouldn't work as Mr H used internet cafes. Lloyds Bank said that Mr H could visit one of its branches and carry out his banking there once he returned to the UK, but that he wouldn't be able to use internet banking in the meantime. Mr H was unhappy and so complained to us.

One of our investigators looked into Mr H's complaint and said that Lloyds Bank hadn't acted unfairly when it made changes to its processes in order to implement strong customer authentication – an important measure to combat fraud. But Lloyds Bank had acted unfairly in Mr H's case because it hadn't offered him an alternative way to authenticate that was viable for him given his particular circumstances. Our investigator recommended that Lloyds Bank pay Mr H £200 in compensation and offer him an alternative way of authenticating that was viable for him. In response, Lloyds Bank offered to update Mr H's address on its system so he'd receive statements in the post allowing him to manage his account. But it said that Mr H wouldn't be able to log into his account unless and until he had a UK number. Mr H was unhappy with Lloyds Bank's response and asked for an ombudsman to look into his complaint. So, that's what I've done.

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 Bank has told us that it made changes to its processes in order to implement new regulations that came into effect in September 2019 that affected the whole banking sector –

namely the Payment Services Regulations 2017 ("PSRs"). Those regulations required payment service providers ("PSPs") to apply strong customer authentication in certain circumstances. Those circumstances are set out in in Article 100 of the regulations which says:

> "A payment service provider must apply strong customer authentication where a payment service user—
>
> (a) accesses its payment account online, whether directly or through an account information service provider;
>
> (b) initiates an electronic payment transaction; or
>
> (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses."

The FCA gave PSPs until March 2020 to implement strong customer authentication for online banking and has given the e-commerce industry until March 2022 to implement strong customer authentication for online payments. The e-commerce industry includes card issuers, payment firms and online retailers. There was, of course, nothing to stop firms bringing in strong customer authentication sooner than that, if they wanted to do so.

The Payment Services Regulations – which implemented an EU Directive from 2015 commonly known as the revised Payment Services Directive – define "strong customer authentication" as:

> "authentication based on the use of two or more elements that are independent, in that the breach of one element does not compromise the reliability of any other element, and designed in such a way as to protect the confidentiality of the authentication data, with the elements falling into two or more of the following categories—
>
> (a) something known only by the payment service user ("knowledge");
>
> (b) something held only by the payment service user ("possession");
>
> (c) something inherent to the payment service user ("inherence");"

In short, strong customer authentication involves, amongst other things, checking that the person accessing a payment account online or initiating an electronic payment is permitted to do so. PSPs have to "authenticate" the person in question using factors based on "knowledge", "inherence" or "possession" and must use at least two independent factors when doing so. They can't, for example, check using only "knowledge" based factors, but they can check using one or more "knowledge" based factors and one or more "possession" based factors. Mr H is unhappy that Lloyds Bank changed its processes – he wants to be able to carry on logging on the way he had done before – and unhappy that the changes involved him having to own his own phone or computer.

Lloyds Bank's approach to implementing strong customer authentication

I don't think it was unfair or unreasonable of Lloyds Bank to implement strong customer authentication – it's an important measure to help combat fraud. Mr H would like to carry on logging onto online banking the way he used to. I can understand why he's said this, but I don't agree with him that I should be telling Lloyds Bank not to implement strong customer authentication measures for his account. I do, however, agree with our investigator that Lloyds Bank needs to offer alternative ways of authenticating that are viable for customers like Mr H. I'd like to explain what the FCA has said about strong customer authentication and its expectations first before saying what I think that means in this case.

What has the FCA said about strong customer authentication and its expectations?

The Financial Conduct Authority (the "FCA") has published several papers about strong customer authentication and its expectations and it has written to firms about this too. In a paper published in June 2019 – "Payment Services and Electronic Money – Our Approach" – the FCA described its approach to the PSRs and payment services and e-money related rules in its Handbook. In paragraph 20.21 of its paper the FCA said:

> "We encourage firms to consider the impact of strong customer authentication solutions on different groups of customers, in particular those with protected characteristics, as part of the design process. Additionally, it may be necessary for a PSP [Payment Service Provider] to provide different methods of authentication, to comply with their obligation to apply strong customer authentication in line with regulation 100 of the PSRs 2017. For example, not all payment service users will possess a mobile phone or smart phone and payments may be made in areas without mobile phone reception. PSPs must provide a viable means to strongly authenticate customers in these situations."

The FCA has, in my opinion, made it clear in its paper and elsewhere that businesses shouldn't rely on mobile phones alone to authenticate their customers and should provide viable alternatives for different groups of customers. The FCA has, in my opinion, also made it clear in this paper and elsewhere that this includes people who don't possess a mobile phone or a smart phone and not just those who can't use one. The FCA has talked, for example, about managing the potentially negative impact of strong customer authentication on different groups of customers "particularly the vulnerable, the less digitally engaged or located in areas with limited digital access". And the FCA has also talked about the need for firms to develop strong customer authentication "solutions that work for all groups of consumers" and has said that this means they "may need to provide several different authentication methods for your customers".

Why is Mr H complaining?

Mr H is complaining about two things, broadly speaking, namely that he doesn't like the fact that Lloyds Bank has changed its processes – he'd rather go back to the "old way" of logging on – and he's not happy with the options Lloyds Bank offers. Lloyds Bank offered four options and, in the course of this complaint, it's accepted that none of them work particularly well for Mr H.

Should Lloyds Bank have done more for Mr H?

One of the options that Lloyds Bank offered relied on Mr H having a UK mobile phone number – that's a problem for Mr H as he was living in France at the time (and still is) and he doesn't use phones as he's hard of hearing. Lloyds Bank has pointed out that Mr H's account is meant for UK residents only, and that there are some services it's unable to offer

non-UK residents, so this wasn't necessarily unfair. I accept some – but not all – of Lloyds Bank's points on this question. Mr H, for example, was clearly eligible when he originally applied for the account. And he didn't have any problems continuing to use it when he moved to France. His problems only started when Lloyds Bank implemented strong customer authentication. More importantly, however, in this case I don't think the question of whether or not Mr H is living in the UK is key. I say that because even if Mr H was a UK resident, there's still the fact that he doesn't use phones as he's hard of hearing. In short, none of the options that Lloyds Bank offer that rely on phones are attractive to Mr H, and understandably so.

Shortly after I started looking into this complaint, Lloyds Bank said that it was planning to introduce an option to authenticate using a "token". I explored the "token" with Lloyds Bank further as it looked like it might solve Mr H's complaint. Having done so, it became clear that the "token" only allows customers to authenticate when they're doing online shopping – it doesn't allow them to authenticate when they're doing online banking. That's important because Mr H is only interested in online banking, so the "token" doesn't help.

Lloyds Bank then offered to help Mr H buy a basic mobile phone – on which he could receive one-time passcodes – and to pay him compensation for the distress and inconvenience he'd experienced in the meantime. I put this offer to Mr H – notwithstanding the fact that I thought he was very unlikely to accept it given that he doesn't want a solution that involves phones or is too technical. He wasn't interested - again understandably so. It means Lloyds Bank hasn't been able to find a solution that works for Mr H.

Putting things right

It's disappointing that Lloyds Bank hasn't been able to find a solution that works for Mr H, particularly in light of what the FCA has said. It means Mr H won't be able to manage his account the way he'd like to. Lloyds Bank have, in the circumstances, offered to pay Mr H £500 in compensation in full and final settlement of his complaint – reflecting the distress and inconvenience he's experienced to date and the fact that he won't be able to manage his account the way he'd like to going forwards. In this particular case, given the overall impact on Mr H, I think this offer is fair.

My final decision

Lloyds Bank PLC has made an offer to pay £500 to settle the complaint and I think this offer is fair in all the circumstances.

So, my decision is that Lloyds Bank PLC should pay Mr H £500 in full and final settlement of his complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr H to accept or reject my decision before 24 October 2022.

Nicolas Atkinson
Ombudsman