DRN-3127699

The complaint

Mr B complains Metro Bank PLC's didn't warn him that it was about to change its processes and, as a result, he wasn't able to update his mobile number or access his account online.

What happened

Mr B has a current account with Metro Bank. He opened the account in 2016 and was living in the UK at the time. He says he had to open the account in order to get a Metro Bank mortgage. He set up a couple of direct debits and made payments towards his credit card – issued by another bank. He says he has a current account with another bank and that his Metro Bank account isn't his main account.

In August 2020 Mr B wanted to log onto his online banking but found he couldn't do so as he needed a one-time passcode in order to log on and the mobile number Metro Bank had for him was out of date. So, he called Metro Bank to update his mobile number – from an old UK mobile number to a foreign mobile number as he was abroad at the time. He answered a number of security questions – all successfully so – and was then asked for the number on the front of his debit card. Mr B said he didn't have his debit card with him – he'd destroyed it as he never used it so felt it was risky keeping it. Metro Bank said that without the number on his debit card it wouldn't be able to update his mobile no. Metro Bank said that the only other way Mr B could update his details was to come into branch – something he said he couldn't do as he was overseas. Metro Bank also said it had updated its processes for online banking and that he'd need a one-time passcode in order to log into his account.

Mr B complained to Metro Bank saying that it hadn't warned him that it was about to change its processes meaning he'd not been able to change his details beforehand and was now unable to access his account. Mr B tried to change his number again after Metro Bank had identified an exceptions process, and was able to add a foreign number to his account which Metro Bank said it was happy to call him on to speak about his complaint, for example. Metro Bank said, however, that in order to log into his online banking or make online payments he'd need to provide a UK mobile number as it could only send one-time passcodes to a UK number. Metro Bank said Mr B could use its telephone banking service as an alternative. Mr B was unhappy with Metro Bank's response – saying that it would be incredibly expensive for him to call from overseas – and complained to us.

One of our investigators looked into Mr B's complaint and said that they thought Metro Bank could have done more to help. Our investigator recommended £100 in compensation. Metro Bank didn't agree and asked for an ombudsman to look into this 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.

Mr B complained to Metro Bank in November 2020 that he wasn't able to access his online banking because Metro Bank was saying he'd need to authenticate using a one-time

passcode sent to a mobile phone – and he didn't have a mobile phone. Mr B complained that this was in breach of clear guidance that the Financial Conduct Authority had issued.

Metro Bank said that it had made changes to its online banking in order to implement new regulations that came into effect in September 2019 – namely the Payment Services Regulations 2017 ("PSRs"). These 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 PSD2 – 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. The changes that Metro Bank made to its processes – and the difficulties they caused Mr B because he's abroad – is at the heart of this complaint.

Metro Bank's approach to implementing strong customer authentication

Metro Bank has, broadly speaking, three ways in which its customers can authenticate, but all of them involve at one stage or another their customer having a UK number. Mr B doesn't think that's fair. Before I say more, it probably helps to explain what the FCA has said on strong customer authentication.

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. The FCA said the paper "provides guidance for a practical understanding of the requirements, our regulatory approach and how businesses will experience regulatory supervision". The FCA added that its "guidance is intended to illustrate ways (but not the only ways) in which a person can comply with the relevant regulations and rules". 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".

Should Metro Bank have done more for Mr B when he originally complained?

Mr B has told us that he doesn't own a UK mobile phone. So I've taken the papers the FCA has published on strong customer authentication and its thoughts – particularly in relation to people who do not possess a mobile – into account when deciding whether or not Metro Bank should have done more when Mr B originally complained and whether or not its actions were fair and reasonable in all the circumstances. In addition, I've taken the Payment Services Regulations – in particular, Article 100 – into account as well as FCA Principle 6 – that firms must pay due regard to the interests of its customers and treat them fairly. I've also taken into account Metro Bank's argument that its accounts are meant for UK residents.

Having done so, I agree with our investigator that Metro Bank could and should have done more here.

Putting things right

Following my involvement, and at my suggestion, Metro Bank agreed to pay Mr B £250 in compensation. Mr B has told me he's happy to accept that on the basis that he'll have to use telephone banking instead.

Metro Bank has said that it is considering exiting its relationship with Mr B as its accounts

are meant for UK residents and Mr B appears to be living abroad. I haven't factored that into this decision as Metro Bank hasn't taken steps to exit its relationship with Mr B. Should it do so, Mr B might complain, and that complaint might come to us. But that would be a new complaint, so I'm going to say no more.

My final decision

My final decision is that I require Metro Bank PLC to pay Mr B £250 in compensation in full and final settlement of his complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 28 October 2022.

Nicolas Atkinson
Ombudsman