DRN-4139339

The complaint

Mr C complains Metro Bank PLC's approach to strong customer authentication means he can't make online purchases unless he has a mobile phone, landline or a similar device. He complains that this is discriminatory and exclusionary and that customers shouldn't be coerced into using mobile phones or devices that aren't free.

What happened

Mr C has a current account with Metro Bank.

In May 2022 Mr C contacted Metro Bank to say that he couldn't make online purchases unless he was able to receive a one-time passcode on his mobile phone or he used its mobile banking app. Mr C complained about this saying that he didn't want to be forced into using a mobile phone in order to make online purchases, or to be forced into buying a landline or another device so he could shop online. He said he wanted Metro Bank to send one-time passcodes to, for example, customer email addresses.

Metro Bank investigated Mr C's complaint and said that it had made these changes to its processes in order to implement strong customer authentication and that it didn't offer any other options. Mr C wasn't happy with Metro Bank's response, so complained to us.

Following our involvement, Metro Bank said that it had plans to introduce an alternative way of authenticating that didn't involve mobile phones – namely sending one-time passcodes to landlines – and it offered Mr C £250 in compensation for the trouble he'd been caused. Metro Bank did so in November 2022.

One of our investigators looked into Mr C's complaint and said that they thought Metro Bank's overall response, including its offer of £250 in compensation, was fair and reasonable. Mr C 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 C complained to Metro Bank in May 2022 that he wasn't able to shop online unless he used a mobile phone because Metro Bank was saying he needed to authenticate using a one-time passcode sent to a mobile phone or through its mobile banking app. Mr C complained that this was discriminatory and exclusionary and that customers shouldn't be coerced into using mobile phones or devices that aren't free. He said Metro Bank should be willing to send one-time passcodes to customer email addresses, for example.

Metro Bank has told us that it made changes to online banking and shopping 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 gave 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 its reliance on mobile phones or a piece of technology that its customers would have to pay for rather than technology that is free and accessible to all – is at the heart of this complaint.

Metro Bank's approach to implementing strong customer authentication

In May 2022 Metro Bank had, broadly speaking, three ways in which its customers can authenticate, but all of them involve at one stage or another their customer having a mobile number. Mr C didn't think that was fair and that he shouldn't need to invest in any device in order to shop online. 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 C when he originally complained?

Mr C has a mobile phone, but he says it's an old one so he can't download any apps. More importantly, however, he's told us that he avoids using his mobile phone as much as possible and doesn't think it's right that businesses like Metro Bank should be forcing people into using their mobile phones more and more in their every-day lives. So, I've taken the papers the FCA has published on strong customer authentication and its thoughts into account when deciding whether or not Metro Bank should have done more when Mr C 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.

Having done so, I agree with our investigator that Metro Bank could and should have done more here when Mr C originally complained. I say that because Metro Bank didn't offer non-mobile options at the time and I don't think it was wholly unreasonable of Mr C to say that he wants to avoid using his mobile phone as much as possible and doesn't think it's right that businesses like Metro Bank should be forcing people into using their mobile phones more and more in their every-day lives. I can see that Metro Bank does now offer options that don't involve using a mobile phone. For example, Metro Bank now offers the option of sending a one-time passcode to landlines. In some cases that might not work. But I have to consider Mr C's case, and his individual circumstances. It's clear, given what he's said, that even though he has a mobile phone and is able to receive and use one-time passcodes sent to that mobile – I've heard him do so on a call to Metro Bank – that he wants a solution that

doesn’t involve a device he has to pay for. That, in other words, includes using a landline to authenticate. In other words, he wants to be able to receive one-time passcodes by email, for example. I can understand why Mr C has said this, but looking at his individual circumstances and considering everything else I’ve mentioned above, I don’t think I can say Metro Bank has acted unfairly or unreasonably here.

Putting things right

Metro Bank agreed – following our involvement – that it could have done more in this case and offered to pay Mr C £250 in compensation to reflect this. I agree with our investigator that the steps Metro Bank has taken are fair and reasonable. So, that’s what I’m going to require Metro Bank to do. Mr C can decide whether or not he wants to accept – if he does, Metro Bank’s offer will become legally binding.

My final decision

Metro Bank PLC has offered to pay Mr C £250 in compensation to settle this complaint and is introducing an alternative way of authenticating that didn’t involve mobile phones. I think this offer is fair in all the circumstances.

So, my decision is that Metro Bank PLC should pay Mr C £250 in compensation.

Under the rules of the Financial Ombudsman Service, I’m required to ask Mr C to accept or reject my decision before 15 June 2023.

Nicolas Atkinson
Ombudsman