DRN-3329485

The complaint

Mr C complains that changes Metro Bank PLC has made to its processes mean he can no longer access his account or carry out transactions as he doesn't own a mobile phone. He also complains that Metro Bank PLC didn't send him hard copy statements when he asked for them meaning he wasn't able to monitor his account.

What happened

Mr C has a current account with Metro Bank.

In November 2020 Mr C complained to Metro Bank that he could no longer access his account or carry out transactions as it had changed its processes – he said the changes meant he needed a mobile phone to verify himself. He was unhappy with this because he didn't have a mobile phone. In the meantime, Mr C asked Metro Bank to send him hard copy statements so that he could monitor his account and make sure he didn't become the victim of fraud.

Metro Bank investigated Mr C's complaint but didn't uphold it. Metro Bank said that it had updated its processes in order to implement strong customer authentication, and it had taken the decision to authenticate by sending one-time passcodes to their customers' mobile numbers. Metro Bank said that it offered another alternative, namely that its customers could "bind" the device they were using for their online banking. In addition, Metro Bank said Mr C could use its telephone banking service or its branches.

Mr C was unhappy with Metro Bank's response saying that it had admitted it was in breach of clear guidelines from the Financial Conduct Authority (the "FCA") on what it expects of firms implementing strong customer authentication as Metro Bank had said the only option its customers had was to receive one-time passcodes to a mobile phone. He was unhappy that Metro Bank still hadn't sent him hard copy statements too. He complained to us.

One of our investigators looked into Mr C's complaint and said that they thought Metro Bank had offered an alternative – Mr C could "bind" the device he was using – but that Metro Bank should have explained to Mr C how to set this up. In addition, our investigator thought that Metro Bank had caused unnecessary distress and inconvenience because it hadn't sent Mr C hard copy statements. Our investigator also asked Metro Bank if it was going to authenticate online shopping transactions in the same way, as Mr C had contacted them to say that Metro Bank was planning on adopting the same system for online shopping, which Metro Bank said it was going to. Metro Bank disagreed with our investigator's recommendations saying that its website explained how to "bind" a device so there was nothing more to explain. Having explored this option further, our investigator said that Metro Bank's process for "binding" a device appeared to involve a one-time passcode sent to a mobile and that this was not, therefore, a non-mobile alternative. Metro Bank remained unhappy with our investigator's recommendations – which included paying Mr C £500 in compensation – saying that it was not our role to say how it run its business as that was the job of the regulator, the Financial Conduct Authority. As Metro Bank disagreed with our investigator's recommendations, I've looked into this complaint.

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 has been using the internet and internet banking for over 20 years. He has a laptop and uses this to access the internet and internet banking. He doesn't own a mobile phone and doesn't want to own a mobile phone.

Mr C 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 C 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 its apparent reliance on mobile phones according to Mr C as a way of authenticating – is at the heart of this complaint.

Metro Bank's approach to implementing strong customer authentication

Metro Bank said in response to Mr C's complaint that it had decided to use one-time passcodes sent to their customers' mobile phones in order to authenticate customers who wanted to log into their online banking. Metro Bank said that an alternative option was when it was comfortable that a login was occurring from a trusted device or browser linked to a genuine person. Metro Bank said that it had no plans at that stage to offer any other alternatives. Metro Bank added that it offered telephone banking via its contact centre, noting that Mr C had recently used that service. And that its stores were an option too. Mr C said that this response amount to an "admission" that Metro Bank had breached clear guidance from the FCA as Metro Bank had said it had no plans to offer any alternatives other than to one-time passcodes sent to their customers' mobile phones. I don't entirely agree – although I will say that I'm satisfied that in order to "trust" a device Mr C would have to be able to receive a one-time passcode. But it probably helps to say more once I've explained 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 told us that he doesn’t own a 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 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.

Putting things right

Following my involvement, Metro Bank agreed to pay the £500 in compensation that our investigator had recommended. In addition, it let us know that it is rolling out a one-time passcode to landline option. I consider those steps to be a fair resolution to this complaint.

My final decision

Metro Bank PLC has offered to pay £500 to settle the complaint and I think this offer is fair in all the circumstances. So, my decision is that Metro Bank PLC should pay Mr C £500.

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

Nicolas Atkinson
Ombudsman