DRN-3846162

The complaint

Mr K complains Bank of Scotland plc's approach to strong customer authentication means that he can't use his online banking when he's away from home.

What happened

Mr K has a current account, a debit card, and a credit card with Bank of Scotland.

Mr K says that he used to use online banking a lot, to check his account and to make payments, particularly when he was abroad. He says that he used his laptop to go online if he was at home – if not he'd borrow one of his family or friend's laptops or tablets.

In March or April 2020, Mr K says that Bank of Scotland made changes to the way its online banking worked. He says that he was told he'd need to enter a one-time passcode sent to a mobile phone registered in his name in order to log into his online banking or make payments. Mr K says that these changes meant he could no longer use his online banking as he doesn't have a mobile phone or want one. He says that this caused him a lot of problems as the changes occurred during lockdown. He says he couldn't check the balance on his account or make payments, and that he had to go into town and use an ATM in order to print out mini statements and check his balance. He says that this put him at risk.

In October 2020, Mr K says that his debit card was retained by an ATM. He says he had to visit a branch because of this and when he did so he discovered that the address Bank of Scotland had on its systems was an old address. He complained to Bank of Scotland about this and about the difficulties he was having using its online banking.

Bank of Scotland investigated Mr K's complaint about his address and accepted in November 2020 that it had updated his address to an old address in error. Bank of Scotland offered him £150 in compensation for the distress and inconvenience this caused. Bank of Scotland also investigated Mr K's complaint about the difficulties he was having using its online banking. Bank of Scotland didn't uphold that part of Mr K's complaint, saying that it had made changes to the way its online banking worked in order to protect his account. Bank of Scotland said that it couldn't send the one-time passcode by email – as Mr K had suggested – as email wasn't a secure way of communicating.

In February 2021 Mr K complained to Bank of Scotland a second time about problems he was having using its online banking. He complained that he was no longer able to access his online banking with his registered name, password and secure phrase. He complained that he now needed a one-time passcode that had to be sent to either a mobile phone or a landline. He said that this meant he had to be near his landline – meaning he had to be at home – in order to do online banking since he didn't have a mobile phone. He also said that he was worried that Bank of Scotland had told him that it intended to introduce the same process for online shopping, meaning he'd soon not be able to do that too. He said that he wanted Bank of Scotland to introduce card readers so that he could authenticate when he wasn't at home, and in particular when he was abroad. Mr K said that the changes Bank of Scotland had made and planned to make were and would cause him a lot of problems as these changes occurred and were going to occur during lockdown. They meant he'd put

himself at risk and would have to continue to do so.

Bank of Scotland looked into Mr K's second complaint about the problems he was having with his online banking and online shopping and said that the changes it had made were designed to protect his account. Bank of Scotland said that he should make sure it had his most up to date number and that he should call the number on the back of his card if any online purchases were declined.

Mr K was unhappy with Bank of Scotland's response, saying it had focussed on explaining why it had introduced strong customer authentication – which wasn't something he'd objected to or complained about – rather than on why it hadn't introduced alternative ways of authenticating that didn't involve a mobile phone or a landline. So, he complained to us saying that he'd soon be travelling abroad again for family reasons and to receive medical treatment and that he'd need to be able to make important payments whilst he was abroad.

Our investigator said that we couldn't look into Mr K's first complaint as he'd referred it to us too late. He said that we could, however, look into Mr K's second complaint. Having done so, our investigator said that Bank of Scotland hadn't acted unfairly as it was making changes to its security processes in order to meet regulatory requirements and had taken a commercial decision to do so. Our investigator said that he could see that the changes had caused Mr K "some inconvenience" because the alternatives that had been implemented weren't ones that he "liked" but that didn't mean Bank of Scotland had acted unfairly.

Mr K disagreed with our investigator saying that the methods Bank of Scotland had made available were discriminatory and unfair towards a considerable (and often vulnerable) part of society. He said people without mobile phones would be severely disadvantaged – particularly people who want to bank from abroad as online banking is the only way that they can do so. He also said that the changes hadn't simply caused him "some inconvenience" – they'd caused him major detriment. He said Bank of Scotland could offer alternatives that other businesses offer – for example, card readers, and that this solution would work for him from any location – at home, at work, visiting friends or travelling abroad. He said that Bank of Scotland already offered card readers, but to customers with business accounts only. He said he didn't think a landline was secure as they might not only be used by the customer. In his case, he said he shared a landline with at least two other people as the landline was in the living room. More recently, Mr K has told us that the impact of being unable to use his online banking – particularly whilst abroad when visiting his family – has become severe because of wider global events. He wanted an ombudsman to look into his complaint. So, that's what I've done.

Last month I issued a provisional decision saying that I was minded to uphold this complaint as I didn't think Bank of Scotland had acted fairly when it said that it wouldn't offer Mr K an alternative way of authenticating that didn't involve a landline or a mobile phone. I said that I agreed with Mr K that the options Bank of Scotland is offering don't work well when he's travelling / not at home and that this, therefore, puts Mr K at a disadvantage because he doesn't own or want a mobile phone. I also said that in this particular case, given that Bank of Scotland told us that it cannot offer any other options, I thought the appropriate remedy was to award compensation to Mr K to reflect the fact that his account and cards, although still useful, aren't as convenient as they used to be because he'll either not be able to use them at times when he's abroad or he'll have to take his laptop – or another device he can trust – with him. I said I considered an award of £250 to be appropriate. I invited both parties to comment on my provisional decision and asked Bank of Scotland to let me know whether it had introduced any further alternative ways of authenticating since we started looking at this complaint. In particular, whether it had introduced or has plans to introduce a token or a card reader option as several businesses have recently done that. I said that if Bank of Scotland had introduced a token or a card reader option, then it would be helpful to know

whether or not that option applies to online banking, online shopping or both.

Both parties responded to my provisional decision. In its response, Bank of Scotland said that it had introduced a "token" that customers could use to authenticate themselves when doing online shopping, but not for online banking. In his response, Mr K said that he'd checked to see whether or not he could download Bank of Scotland's mobile app to his laptop and he can't. He also said that he didn't think the award I was minded to make would motivate Bank of Scotland to make changes, that I should consider making an ongoing award and that an award of between £3,000 to £5,000 would more accurately reflect the impact on him of not having had access to his online banking for over three years.

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.

Bank of Scotland told Mr K that it had made changes to the way online banking and online shopping worked and said that these changes were designed to protect his account. Bank of Scotland told Mr K that the changes were as a result of new regulations that were going to come into effect in September 2019 that affected the whole banking sector.

Bank of Scotland is right that new regulations making changes to the way businesses authenticate came into effect in September 2019 – the Payment Services Regulations 2017 ("PSRs"). Bank of Scotland is also right that these regulations affected the whole banking sector. The 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 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. The way Bank of Scotland has gone about those checks – and what that means for Mr K when he's not at home – is at the heart of this complaint.

Bank of Scotland approach to implementing strong customer authentication

Bank of Scotland has told us that it's made changes to how customers log into its website and shop online as a result of new regulations. Bank of Scotland has told us that it now uses two factor authentication to identify its customers and that this involves using two out of three different types of identification:

- something you know (password / memorable information);
- something you have (a device you own e.g. mobile phone or laptop);
- something you are (biometrics like fingerprint or face scanning).

Bank of Scotland has told us that Mr K had three ways to authenticate, namely:

- he could label a device he owned as "trusted" and Bank of Scotland would recognise this as his usual internet device. Bank of Scotland has explained that this setting would be stored as a cookie on his device, so it's important it doesn't get deleted. He'd log on with his user ID, password and memorable information as normal;
- Bank of Scotland could send a code to a registered mobile phone which he could enter along with his user ID, password and memorable information;
- Bank of Scotland could phone a registered landline and would give him a code number on screen that would need to be keyed into his telephone handset.

In other words, Bank of Scotland has told us that Mr K had to pass a "knowledge" based check (his password and memorable information) and a "possession" check (either using a trusted device or receiving a code on his mobile phone or his landline and keying it in). Bank of Scotland's approach has developed since 2020 – that's true of many businesses – and I've said more about this later on.

Why did Mr K complain?

Mr K has told us that he doesn't own a mobile phone, and he doesn't want one. He has access to a landline when he's at home, but he lives with other people and the landline is in the living room, so he doesn't feel it's particularly safe. More importantly, he used to rely on online banking when he travelled or was away from home, so sending a one-time passcode to that landline doesn't help as he wouldn't be there to receive the code. He's also told us that he a laptop (although he hasn't made it a trusted device) but that it's neither practical nor reasonable for him to carry his computer with him when he travels just for the sake of having a trusted device not least because it would take up considerable space and weight in

his luggage. He's told us he usually uses computers and devices of friends or acquaintances when he travels, or public computers in libraries and internet cafes. He knows that those aren't the type of devices that should be made trusted devices.

It's clear from what Mr K has told us that his main complaint about Bank of Scotland's approach to strong customer authentication is that it doesn't allow him to access his online banking when he's travelling or away from home. He's able to access his online banking when he's at home, as he has a landline to which codes can be sent, but as he rightly points out this only works when he's at home and not when he's abroad or travelling.

Mr K isn't complaining about Bank of Scotland's decision to introduce strong customer authentication, which is an important measure designed to combat fraud, and one that PSPs are obliged to implement. And he's not complaining about having to complete additional checks either. He agrees that strong customer authentication is an important measure designed to combat fraud. I'm satisfied that the only reason why Mr K complained was because he didn't feel Bank of Scotland had offered a method of authenticating that would allow him to continue to access his online banking when he's travelling or away from home. He wouldn't have complained had Bank of Scotland, for example, offered him the option of authenticating using a card reader or a token. I'll come back to this later as I asked Bank of Scotland if it had introduced a card reader and / or a token option or had plans to do so since Mr K originally complained as I know a number of businesses have recently done so.

Bank of Scotland's approach to strong customer authentication - now

Bank of Scotland's approach to strong customer authentication has developed since Mr K originally complained. Bank of Scotland, like many other businesses, has, for example, now extended strong customer authentication to online shopping. That means that when one of its customers, for example, puts their debit or credit card into a website in order to make an online purchase, Bank of Scotland will sometimes check that the person who has done that is their customer using strong customer authentication. Bank of Scotland also now offers the option of its customers authenticating using its mobile banking app. That means customers can, for example, authenticate using their fingerprint or their face, amongst other things. In other words, Bank of Scotland now offers the option to its customers of authenticating using the "inherence" factor. Bank of Scotland told us that its mobile banking app isn't an app that can only be downloaded onto a mobile phone. It told us that it can be downloaded onto any mobile device – including potentially a tablet and / or a laptop. In his response to my provisional decision, Mr K said he'd tried to download the app onto his laptop but hadn't been able to do so and pointed out that Bank of Scotland's website listed certain requirements that had to be met in order to download the app which his hardware and software didn't meet. He said he'd still need a mobile number to complete this process. I've taken these comments into account.

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 Bank of Scotland have done more for Mr K when he originally complained?

Mr K 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 Bank of Scotland should have done more when Mr K 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 taken everything into account, I don't think it was unfair or unreasonable of Bank of Scotland to implement strong customer authentication – it's an important measure to help combat fraud. Nor do I think it was unfair or unreasonable of Bank of Scotland to decide that it was going to rely on "knowledge" and "possession" when authenticating its customers (it's since offered "inherence"). I do, however, agree with Mr K that Bank of Scotland needed to provide its customers with an alternative to a mobile phone in order to prove possession. Bank of Scotland offered two alternatives at the time, namely asking its customers to key a code that would be displayed on screen into their landline when Bank of Scotland called and allowing its customers to "trust" a device they own.

I agree with Mr K that a landline might not always be the safest way to authenticate a customer in that there's no guarantee that only the customer has access to it. And I accept, for example, that his landline is one he shares with other people and is in a communal area – a living room. But I don't think I can say it's unfair or unreasonable that Mr K has to use his landline to authenticate if he wants to use his online banking or do online shopping at home not least because the code is only useful if the person who receives it also has other details needed to complete the transaction to which the code relates. More importantly, Mr K is clearly far more concerned about being able to use his online banking or do online shopping when he's not at home.

Mr K has a laptop that only he has access to which he could label as a "trusted device". He's told us that he hasn't done this, but I've seen nothing to suggest that he wouldn't be willing to do so. Mr K has instead said that it's neither practical nor reasonable for him to carry his computer with him when he travels just for the sake of having a trusted device not least

because it would take up considerable space and weight in his luggage. He's told us he usually uses computers and devices of friends or acquaintances when he travels, or public computers in libraries and internet cafes.

The FCA has said – and I think it's fair and reasonable – that in its view firms should be giving their customers several different ways to authenticate themselves, and not just rely on mobile phones, so that authentication works for all groups of consumers. I can see why the FCA said this – as its paper makes clear, not everyone owns a mobile phone, nor is everyone able to use a mobile phone. So, it's important that these groups aren't overlooked otherwise they could find that they're unable to access online banking or make online payments or manage their accounts remotely. And these aren't the only groups potentially affected. Or the only scenarios when authentication can be problematic, depending on the solution adopted.

I accept that Mr K used to use his online banking a lot when he wasn't at home – particularly when he travelled abroad – and I've no reason to believe the same won't be true for his online shopping. I accept that a card reader or a token that would allow Mr K to generate a code in these circumstances would be extremely helpful for Mr K as they would allow him to log into his online banking or do online shopping wherever he happened to be – as long as he had internet access where he was because without that he wouldn't be able to get online. Mr K has given us a number of examples where he's tried and failed to use his online banking when he's not been at home. He will, of course, only have to worry about strong customer authentication when he is online – either to access his account or to make a payment or to shop. If he used his laptop to go online, then that's a device that I'm satisfied he can trust. As I said in my provisional decision, I don't think that's unreasonable. I remain of that view. It does, however, mean that Mr K would have to have his laptop – or a device he could trust – with him when he travels if he wants to be able to authenticate. If his laptop or device was the only way he'd be able to get online when he's travelling – given that it's only when he online that he needs to be able to authenticate – then I don't think that this would be unreasonable. But I'm satisfied that there are a number of ways that Mr K can go online without his laptop or a device of his own – he's given several examples, mostly involving shared devices in relation to which saving cookies isn't recommended. In the circumstances, I agree with Mr K that the options Bank of Scotland is offering don't work well when he's travelling / not at home and that this, therefore, puts Mr K at a disadvantage because he doesn't own or want a mobile phone. In my provisional decision I said that in this particular case, given that it appeared Bank of Scotland couldn't offer any other options, I thought the appropriate remedy was to award compensation to Mr K to reflect the fact that his account and cards, although still useful, weren't going to be as convenient as they used to be because he'll either not be able to use them at times when he's abroad or he'll have to take his laptop – or another device he can trust – with him. I said I considered an award of £250 to be appropriate.

In its response, Bank of Scotland let me know that it had introduced a new way for its customers to authenticate when they're doing their online shopping. My understanding is that Bank of Scotland has introduced a token, but the response on this case suggests it might be a card reader. Ultimately in this particular case I don't think it matters whether it's a token or a card reader as I'm satisfied Mr K could use either. It means I'm satisfied that Mr K won't have difficulties doing online shopping when he's not at home even if he chooses not to make his laptop a "trusted device" or decides that his laptop is too heavy and bulky to carry with him when he travels. The token / card reader won't, however, help him authenticate if he wants to do his online banking when he's not at home. I know that's important to Mr K and that the only option that will work for him – because he doesn't own a mobile phone – is taking a "trusted device" with him which isn't entirely convenient. In the circumstances, I remain of the view that I should, in this particular case, award compensation to reflect the fact that his account and cards, although still useful, aren't going

to be as convenient as they used to be because he'll either not be able to use them at times when he's abroad or he'll have to take his laptop – or another device he can trust – with him.

Putting things right

Mr K would like me to make an award that will motivate Bank of Scotland to make changes. I can understand where he's coming from, but that's not the purpose of the compensation awards we make. Our awards are to compensate for distress and inconvenience. He'd also like me to make an award of between £3,000 and £5,000 having set out in detail the different ways in which not being able to manage his accounts has impacted him.

I've thought about what Mr K has said and about the options that he now has. Having done so I remain of the view that an award of £250 is fair, so that's the award I'm going to make. I've taken into account the fact that I'm only looking at Mr K's second complaint – in other words the one he made in February 2021 as his first complaint was referred to us out of time – when making this award.

I hope that both parties will now speak to each other so that Mr K is able to set up a "trusted device" and get himself a token or a card reader. It would be helpful if Bank of Scotland could also show Mr K how to download its mobile app onto his laptop using his landline, if needs be and if possible, to complete that process assuming this is possible.

My final decision

My final decision is that I require Bank of Scotland plc to pay Mr K £250 in compensation to reflect the fact that his account and cards, although still useful, aren't as convenient as they used to be.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr K to accept or reject my decision before 19 January 2023.

Nicolas Atkinson
Ombudsman