DRN-4301001

The complaint

Ms S complains that Bank of Scotland plc trading as Halifax won't exempt her from strong customer authentication.

What happened

Ms S has a current account with Halifax with a debit card. She's been a customer of Halifax for many years.

Ms S has told us that she's largely housebound and has a number of disabilities and vulnerabilities which mean that she avoids screens and going online, amongst other things. She's also told us that she used to do the majority of her shopping over the phone in order to avoid screens and going online. That included ordering food over the phone from a well-known supermarket.

Following the introduction of strong customer authentication, Ms S says that retailers – including the supermarket she orders food from – started saying that they'd need to authenticate her payments when she placed orders over the phone. Ms S complained to Halifax saying that she didn't have a mobile phone in order to receive the one-time passcode she'd need in order to authenticate and that she couldn't retrieve a one-time passcode from her landline at the same time as she was using it to place an order. She complained that she was being pushed into shopping online – and forced into using screens – and asked to be exempted from strong customer authentication.

Halifax looked into Ms S's complaint and said that it could send one-time passcodes to her landline, or she could grant a trusted member of her family power of attorney over her account, so she didn't need a mobile phone in order to authenticate. It also said that it couldn't exempt her from strong customer authentication. And Halifax said, in any event, that it could see Ms S had been authenticating successfully.

Ms S was unhappy with Halifax's response and complained to us. She said she couldn't retrieve one-time passcodes from her landline if she was using it to place an order. And if she was using her iPad to place an order, she'd have to go from her bedroom to her living room and back again to retrieve one-time passcode. She said she'd tried doing this in the past and had fallen and hurt herself. And having a landline in her bedroom wasn't an option. She also said that the times when she'd authenticated successfully were when her family members had helped out, but that was increasingly not an option.

One of our investigators looked into Ms S's complaint and asked Halifax whether or not it would be prepared to offer Ms S a "token" with which she could authenticate herself when shopping online. Halifax agreed to do so. Our investigator thought that the token was a reasonable alternative way for Ms S to authenticate herself in the event that she needed to shop online. But they also felt an award of £350 was appropriate, so that recommended Halifax pay that too. Ms S disagreed, saying it would mean she'd have to use a device with a screen. In short, Ms S didn't agree with our investigator's recommendations and asked for her complaint to be referred to an ombudsman. So, 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.

In July 2023 I issued a provisional decision saying that I was minded to uphold this complaint. Here's what my provisional decision said:

> *"Halifax has told us that it's changed its online banking and the way its website worked. Halifax told Ms S that these changes were as a result of new regulations that came into effect in September 2019 that affected the whole banking sector.*
>
> *Halifax is right that new regulations making changes to the way businesses authenticate came into effect in September 2019 – the Payment Services Regulations 2017 ("PSRs"). Halifax 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 Halifax has gone about those checks and the implications for Ms S's ability to shop and manage her account independently is at the heart of this complaint.

Halifax approach to implementing strong customer authentication – in May 2022

Halifax explained to Ms S in its final response in May 2022 that it had made changes to online banking and online shopping as a result of new regulations. Those changes involved asking its customers to use two factor authentication to identify themselves using two out of three different types of identification, namely:

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

Typically, that would involve Halifax sending a one-time passcode to a customer's mobile phone or landline, to be used in conjunction with their password and memorable information. In other words, passing a "knowledge" based check (password and memorable information) and a "possession" check (receiving a code on a mobile phone or landline and keying it in). Halifax's approach has developed since May 2022 – more on that later.

Why did Ms S complain?

Ms S complained because she says she couldn't order goods over the phone anymore following the changes Halifax made to its processes. Instead, according to Ms S, she was being forced online / into using screens in order to shop for food and other items. Ms S says that being forced online / into using screens has a massive impact on her physical and mental wellbeing given her disabilities and vulnerabilities.

It's clear from what Ms S has told us that she does not want strong customer authentication applied to her, does not want to have to go online and wants to avoid screens.

Halifax's approach to strong customer authentication - now

Halifax's approach to strong customer authentication has developed since Ms S originally complained in May 2022. Halifax, for example, now offers the option of its customers authenticating using a "token". This is a device that doesn't rely on a mobile signal, but it is a device with a screen.

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 Halifax have done more for Ms S when he originally complained?

Ms S 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 Halifax should have done more when Mr W 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 Halifax to implement strong customer authentication – it's an important measure to help combat fraud. Nor do I think it was unfair or unreasonable of Halifax 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 Ms S that Halifax needed to provide its customers with an alternative to a mobile phone in order to prove possession. Halifax did offer an alternative – a landline – at the time and it now offers "tokens". Ms S have given good reasons why using her landline or a "token" wouldn't work, and I accept that neither of them are good options for her. There is, however, a more fundamental issue in this case, and it's that issue that I want to turn to now.

Ms S's fundamental issue

Halifax said when it looked into Ms S's complaint that it could see she'd been authenticating successfully and that it couldn't exempt her from strong customer authentication. I've told Halifax that I'm satisfied that Ms S hasn't been authenticating herself, and that the occasions when there have been successful authentications have been down to help from family and friends, and sometimes neighbours. In other words, I'm satisfied that she can't authenticate independently. Ms S has told me that her family and friends no longer want to help her – they're moving increasingly away from online banking – and her circumstances and her family's circumstances mean that they're less able to. But the more important point here is that Ms S should be able to operate her account independently. In this particular case, it doesn't feel right Halifax telling Ms S to appoint someone as her power of attorney. For that reason, I asked Halifax to consider exempting Ms S. Halifax said two things in response.

Firstly, Halifax said that if the only thing Ms S wants to do is place orders over the telephone using her card, then there's no need to exempt her from strong customer authentication as orders placed over the telephone aren't caught by strong customer authentication. Having looked into this further, Halifax said that it appears that the supermarket, for example, where Ms S orders her food from over the phone is processing her order through its online system giving the appearance that she's using her debit card online when that's not what she is trying to do. I'll return to this in a moment.

Secondly, Halifax said that it can't remove the requirement for strong customer authentication. I've already said to Halifax that I don't necessarily agree that this is the case and that it appears to be inconsistent with a paper UK Finance produced in October 2021. In that paper, UK Finance had the following to say at paragraph 20:

> *"20. Vulnerable customers*
>
> *20.1 UK Finance recognises that there will be certain customers in relation to which the application of SCA will present a number of challenges. These include vulnerable customers, defined by the FCA as somebody who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care.*
>
> *20.2 UK Finance has set out below its views on how considerations vis-à-vis vulnerable customers should be applied with respect to two specific SCA-related matters. However, as a general principle, UK Finance's view is that where, having exhausted all of its existing solutions to apply SCA taking into account the customer's potential vulnerability, an issuer cannot physically apply SCA, then the issuer may apply one SCA factor where possible (to complete the transaction) or where this too is not possible, execute the particular electronic transaction or take the particular action nonetheless. It is expected, however, that the issuer will apply some fraud risk mitigation measures (i.e. risk-based assessments of individual transactions, declining high risk transactions) and monitor the level of fraud, adjusting its approach as necessary."*

In short, UK Finance's paper recognises that the harm of excluding particularly vulnerable customers from being able to manage their finances can outweigh the potential risks posed by fraud. I asked Halifax why it didn't think it could exempt Ms S in light of what UK Finance had said and was told Halifax would look into this and get back to me. To date, Halifax hasn't done so. So, I'm going to require Halifax to tell me whether, in light of everything I've said and the additional enquiries it has made, its position has changed and whether it's now willing to exempt Ms S from strong

customer authentication. In relation to this, I want to add one final point.

Halifax has said that Ms S shouldn't need to go through strong customer authentication if all she is doing is placing orders on the phone. I accept that this is all Ms S is trying to do. She doesn't use online banking – if she needs to move money she uses telephone banking – and she doesn't want to be forced into online shopping. I accept too that it's more than likely the way the retailer is processing orders that is making them appear to be online shopping orders. I can, however, only look at Halifax's part in this – given that it's a regulated business providing a financial service. In this particular case, however, given that Halifax has said that Ms S shouldn't need to go through strong customer authentication as all she's doing is placing orders on the phone, I don't think it's unfair or unreasonable to require Halifax to exempt her so that she's in the position she would have been had it not been for the actions of the retailer. I say that because Halifax has the ability to make a difference here, and Halifax is the only entity involved who we have jurisdiction over.

I cannot require Halifax to do something it isn't able to do. In such cases if I think the business hasn't been fair or reasonable compensation for the distress and inconvenience is the only real remedy available to me. So, in the event that Halifax says that it cannot exempt Ms S from strong customer authentication, I'm minded to award compensation to reflect the impact this is going to have on Ms S's ability to manage her account and the fact that she may have to move banks. I'm minded to award Ms S £1,000 in compensation. Our investigator said that they thought an award of £350 was appropriate, but that was on the assumption that Halifax had offered a reasonable alternative. If Halifax says it can exempt Ms S, then I'd be minded to make an award of a similar size to the one our investigator made.

My provisional decision

My provisional decision is that I'm minded to uphold this complaint and require Bank of Scotland plc trading as Halifax to pay Ms S £1,000 in compensation in full and final settlement of this complaint, unless Bank of Scotland plc trading as Halifax confirms in response to this provisional decision that it can exempt Ms S."

I asked both parties to comment on my provisional decision. I didn't hear back from Ms S, but I had spoken to her on the phone and explained what I was minded to say and she was happy with that. Halifax replied saying that it could exempt Ms S but it could only apply an exemption to a particular card, meaning that Ms S would have to ask for any new card to be exempted if her existing card was lost or stolen or expired. Halifax also asked for an extension so that it could speak to stakeholders in the group it belonged to as it hadn't exempted a customer before and so wanted to be able to think everything through. I agreed to an extension. I have not, however, heard back from Halifax despite that extension having expired a while ago and despite emailing several times for an update. So, I'm now going to issue a decision based on everything I've been sent to date.

Putting things right

In its response Halifax confirmed to me that it could exempt Ms S from strong customer authentication even though the process wasn't as straightforward as it could be. I've seen nothing from Halifax to suggest that it's changed its mind. I'm, therefore, going to require Halifax to exempt Ms S from strong customer authentication.

In my provisional decision, I said I'd require Halifax to pay Ms S £1,000 in compensation if it couldn't exempt her to reflect the impact strong customer authentication was going to have on her ability to manage her account and the fact that she may have to move banks.

Alternatively, if Halifax said it could exempt her, I said that I would be minded to make an award similar to the one our investigator made - £350 – which was on the assumption that Halifax had offered a reasonable alternative. It's clear from what Halifax has said that exempting Ms S won't be as straightforward a process as it could be. So, Ms S is likely to still see an impact – albeit a lesser one – on her ability to manage her account.

Given everything I've just said, I consider an award of £500 – along with exemption – to be a fair outcome as that reflects the fact that although exempt Ms S will continue to be impacted. So, that's the award I'm going to make.

My final decision

My final decision is that I'm upholding this complaint and requiring Bank of Scotland plc trading as Halifax to pay Ms S £500 in compensation and exempt her from strong customer authentication in full and final settlement of this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Ms S to accept or reject my decision before 12 September 2023.

Nicolas Atkinson
Ombudsman