DRN-3846837

The complaint

Mr W complains Bank of Scotland plc's (trading as "Halifax") approach to strong customer authentication means that his "internet account" is no longer truly an "internet account". He says that means there are times when he won't be able to use his account when he should be able to.

What happened

Mr W has a credit card account with Halifax with a credit limit of £12,000. He also has a current account with another bank who allow him to authenticate using a token.

In May 2019 Halifax wrote to Mr W to let him know that it was going to be making changes to the way it authenticated its customers. Halifax asked Mr W for his mobile number. Mr W wrote back to Halifax in June 2019 saying that he did not have, nor want, a mobile phone so he couldn't provide them with a number. He also asked how Halifax intended to maintain its internet banking service. In his letter he said why he didn't think its internet banking service would provide an adequate service if it relied on customers having a mobile phone or receiving SMS messages. He also suggested ways Halifax could maintain its internet banking service, including taking advantage of card readers and existing card technology. He has a background in telecommunications.

In November 2020 Mr W wrote to Halifax to complain that he'd had to use a one-time passcode sent to his landline in order to access his account online. He said that he had an "internet based" account because he needs to be able to use it all over the world, particularly when he travels. And that having to rely on his landline meant his account was no longer an "internet based" account. He said that the consequences of him not be able to access his account could be catastrophic.

Halifax investigated Mr W's complaint and said that it provided a number of alternatives, including sending one-time passcodes to a landline, taking advantage of trusted device technology and its mobile banking app. In short, Halifax thought it had done enough. Mr W disagreed saying that these solutions wouldn't work if he was, for example, travelling as they all relied on a phone or the customer not clearing cookies. He ultimately complained to our service. He told us that it is simply impossible to travel in the modern world without a reliable credit card to conduct internet transactions and being able access your account. He said for example that many bookings and payments now can only be made online.

One of our investigators looked into Mr W's complaint but didn't uphold it. They said that they thought Halifax had provided viable alternatives to a mobile phone. Mr W disagreed, saying that unless and until Halifax provided an alternative that worked when its customers had internet access only then there would be times when he wouldn't be able to use his online banking or make online payments. For example, when travelling abroad. So, I was asked to consider his 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.

Having looked into this complaint, I issued a provisional decision. In my provisional decision I said the following:

"Halifax told Mr W that it was making changes to its online banking and the way its website worked. Halifax told Mr W that these changes were as a result of new regulations that were going to come 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 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 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 none of the alternatives it offers being location and technology agnostic according to Mr W – is at the heart of this complaint.

Halifax approach to implementing strong customer authentication – in 2020

Halifax explained to Mr W in its final response in December 2020 that it would be making changes to how customers logged into its website as a result of new regulations. Halifax told Mr W that it would be using two factor authentication and that this was a way that customers could identify themselves 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).*

Halifax told Mr W that there were three options to choose from, namely:

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

In other words, Halifax told Mr W that he'd soon have 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). Halifax's approach has developed since 2020 – that's true of many businesses – and I've said more about this later on.

Why did Mr W complain?

Mr W has told us that he has a number of "internet accounts". He's also told us that he opened these accounts because it's important to him that he's able to manage his finances "over the internet" – that, according to Mr W, is what an "internet account" should by definition allow you to do. He's given us lots of reasons why people generally, including himself, like to open "internet accounts". For example, the convenience of being able to manage your finances online compared to the inconvenience of having to call your bank or visit a branch (particularly during Covid and in light too of the number of branches that have closed over the past few years and continue to close).

Mr W has told us that during his career he's worked in a number of different countries, often for months at a time, and that being able to manage his finances when he's away was important too. He's told us that he's now looking forward to retirement, and that having saved up during his life, he's now looking forward to spending the money that he's put to one side. He's told us that he has plans, for example, to be away for six to twelve months travelling around New Zealand and Australia. And that it will be important that he's able to manage his finances when he's abroad for that long period of time, and other

trips he has planned.

Mr W has told us that he doesn't own a mobile phone, and he's explained why even if he did it wouldn't help him manage his finances. He makes a lot of good points. He's also told us that he owns a computer – this is the device he uses when he's at home – and that the computer he owns at the moment is a laptop.

It's clear from what Mr W has told us that his main complaint about Halifax's approach to strong customer authentication is that it simply doesn't allow him to manage his finances when he's travelling. 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 whenever he has access to the internet. In the circumstances, I can see why Mr W says that his "internet account" is no longer operating like an "internet account" because of the way Halifax has approached strong customer authentication.

Mr W isn't complaining about Halifax'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's agrees that strong customer authentication is an important measure designed to combat fraud. I'm satisfied that the only reason why Mr W complained was because he didn't feel Halifax had offered a method of authenticating that would allow him to continue to operate his account as an "internet account". He wouldn't have complained had Halifax, for example, offered him the option of authenticating using a card reader or a token. I'll come back to this later as I know a number of businesses have recently introduced card readers and tokens and I'd like to know if Halifax has done so too or plans to do so.

Halifax's approach to strong customer authentication - now

Halifax's approach to strong customer authentication has developed since Mr W originally complained in November 2020. Halifax, 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 credit card or debit card into a website in order to make an online purchase, Halifax will sometimes check that the person who has done that is their customer using strong customer authentication. Halifax 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, Halifax now offers the option to its customers of authenticating using the "inherence" factor. It's important to say that Halifax's mobile banking app isn't an app that can only be downloaded onto a mobile phone. It can be downloaded onto any mobile device – including potentially a tablet and / or a laptop.

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 Mr W when he originally complained?

Mr W 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. I'm very confident Mr W doesn't think so either. 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 Mr W that Halifax needed to provide its customers with an alternative to a mobile phone in order to prove possession. Halifax offered two alternatives at the time, namely asking its customers to key a code that would be displayed on screen into their landline when Halifax called and allowing its customers to "trust" a device they own.

I don't think Mr W can say that Halifax hasn't offered him a viable alternative for when he's at home because one of the alternatives it offers is authenticating using a landline – and Mr W has a landline at home which he's able to use. I accept that this isn't true "internet banking" as far as Mr W is concerned as it means he has to rely on his landline and can't just rely on the internet. But I don't think I can say it's unfair or unreasonable that Mr W has to use his landline to authenticate if he wants to log onto his credit card account or use his credit card online at home. I should add that he can also log onto his credit card or use his credit card online when he's at home without having to rely on his landline if he uses the laptop he's told us he has. He'd have to label his laptop a "trusted" device in order to do so, and that means he'd have to be willing to allow a cookie from Halifax to be stored on his laptop. Mr W has told us that he deletes his cookies every time he closes a browsing session, and that this is something anyone who is careful with

security and interested in privacy should do. To the extent that Mr W is talking about browsing on a shared device, I agree with him. But I don't necessarily agree with him when it comes to a private device that isn't shared, as appears to be the case with his laptop. Our investigator suggested he could choose which cookies on his computer to delete. Mr W didn't think this was possible – and that he'd have to delete all cookies or none – and it's probably not something he'd particularly want to do. I've looked into this myself, and I'm satisfied that Mr W can choose which cookies he wants to delete. So, I'm satisfied he has two options when he's at home – relying on his landline or "trusting" his laptop and being selective about the cookies he deletes. I don't think that's unfair or unreasonable.

I accept that asking Mr W to key a code that would be displayed on screen into his landline isn't an option that would work when he's not at home. So, I have to consider whether Halifax has given Mr W a viable alternative to use when he's not at home and, in particular, when he's travelling abroad. I also have to consider whether Halifax has to give Mr W a viable alternative in those circumstances. And, having done so, and having taken everything else into account, I have to decide whether what's happened here is fair and reasonable in all the circumstances or not. So, that's what I'm now going to do.

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. Mr W, given his background, is perhaps more knowledgeable than many when it comes to potential pitfalls here. He's worried, in particular, about what's going to happen when large numbers of people (including himself) start to travel again. And he's worried too about some of the technologies that businesses are relying on – some of which he says are unreliable (because they were never designed to be used the way they are now being used) and some of which he says will soon be redundant. He's told us that many businesses, including Halifax, are relying on "sunny day" solutions, by which he means solutions that work when everything is well, but break down easily. He's told us that this is because businesses, including Halifax, haven't focussed on what's key here – and that, according to Mr W, is making sure at least one solution works whenever a customer has internet access. I can see that there has been a lot of discussion about consumers who might live or work in areas of limited mobile reception, and some discussion about what happens when consumers travel abroad to the EU and beyond – particularly the implication of roaming charges, for example. I agree with Mr W that this might well be an issue that will cause problems in the future, and it would have been helpful to have more material here which I could have considered on how far businesses need to go. But I also have to remember that I am looking at this individual complaint and have to decide what's fair and reasonable in all the circumstances.

Mr W has a credit card with Halifax. That's a card that he can use whenever and wherever he wants – either online or in person as long as the card is accepted where he wants to use it. If he uses it to pay for goods and services when he's present, Halifax won't need to check it's him who's using the card using strong customer authentication as the rules don't apply to what are known as "cardholder present" transactions. That's important to remember. There are, however, likely to be many scenarios when Mr W will want to either log into his credit card account (potentially to check how much available credit he has or to make sure there are no transactions he doesn't recognise) or use his

credit card online when he won't be at home. I accept that a card reader or a token that would allow Mr W to generate a code in these circumstances would be extremely helpful for Mr W as they would allow him to log into his credit card or use it online 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 W hasn't been able to give us any examples of when he's been unable to log onto his account or use his credit card online – although he has been able to give me an example of when he had a problem at an airport because another card he had got blocked on account of security checks. Mr W has said to us that the way he's operated his accounts in the past isn't relevant – he says the only thing that's relevant is how he wants to operate his accounts. I agree with Mr W to a degree. It's clear that he's moving from a period in his life when he worked and has saved to a period in his life when he's likely to want to spend his money and is likely to travel abroad far more and for long periods of time. So, what he's done in the past is likely to be less relevant. I do, however, think I can and should take into account the type of account he has, and how it can be used. In this case, as I've said, he has a credit card which he can use whenever and wherever he wants, as long as the card is accepted. And I also think I can and should take into account how he's used the account in the past and how he's likely to do so in the future.

Mr W will only have to worry about strong customer authentication when he is online – either to access his account or to make a payment. If he uses his laptop to go online, then that's a device that I'm satisfied he can trust – this would mean not deleting all cookies every time he logged off. I don't think that's unreasonable. It does, however, mean that Mr W would have to have his laptop – or a device – 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 W 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 W that the options Halifax is offering don't work well when he's travelling / not at home and that this, therefore, puts Mr W at a disadvantage because he doesn't own or want a mobile phone. In this particular case, however, given that Halifax told us that it cannot offer any other options, I think the appropriate remedy is to award compensation to Mr W to reflect the fact that his credit card, although still useful, isn't as convenient as it used to be because he'll either not be able to use it at times when he's abroad or he'll have to take his laptop – or another device he can trust – with him. I consider an award of £250 to be appropriate.

As I've already mentioned, I'm aware several businesses have recently introduced a token or a card reader option to allow customers to authenticate. I'd like Halifax, when it replies to this provisional decision to let me know whether it has introduced any further alternative ways of authenticating since we started looking at this complaint. In particular, whether it has introduced or plans to introduce a token or a card reader option as several businesses have recently done that – including a token or a card reader that allows customers to authenticate when they're shopping online. In the event that Halifax has introduced a token or a card reader option, then I'd reconsider the award I'm minded to make as it would mean Mr W's card remains as convenient as it used to be."

Both parties were invited to respond to my provisional decision, and both did.

Halifax accepted my provisional decision – including agreeing to pay Mr W £250 in compensation. Halifax also let me know that it had recently introduced a token that would enable Mr W to authenticate online card payments wherever he has an internet connection.

Halifax ordered a token for Mr W which he's since received. The token doesn't, however, allow Mr W to log into his account online – for that he'd still need to use the methods I mentioned in my provisional decision or find alternatives. In response to my provisional decision, Mr W gave detailed reasons why he wouldn't be able to use his laptop to access his account online, meaning that he wouldn't be able to check his balance or his account for fraud in the way I thought he might be able to.

Putting things right

Having reconsidered everything again, I agree with Mr W that his credit card isn't going to be as useful as it used to be when he's travelling. He won't be able to easily check his balance, for example. Fortunately, now he has a token, he will be able to use his card online when he's travelling. I think the token and the £250 compensation that I recommended – and Halifax has accepted – is, however, a fair outcome in overall terms. So, given that Mr W has already received his token, I am going to require Halifax to pay Mr W £250 in compensation in full and final settlement of this complaint. I appreciate that this isn't necessarily the outcome that Mr W was hoping for, but I don't think I can require Halifax to do more.

My final decision

My final decision is that I require Bank of Scotland plc trading as Halifax to pay Mr W £250 in compensation to reflect the fact that his credit card, although still useful, isn't as convenient as it used to be.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr W to accept or reject my decision before 4 January 2023.

Nicolas Atkinson
Ombudsman