DRN-3385165

The complaint

Mr B complains that he needs to have a mobile phone to use Santander UK Plc's online banking services. He's told us that his lifestyle does not require a mobile phone. He thinks it's unfair of Santander to deny him access to online banking services because of this.

What happened

In March 2019 Mr B was unable to make a large payment to an existing payee using Santander's online banking. This was because he'd not signed up to receive one-time passcodes (OTPs) to a registered mobile phone to authenticate payments.

Mr B was able to complete the payment over the phone, but he complained that although he didn't mind the inconvenience of having to use telephone banking on "*rare occasions*", he was concerned about Santander's plans to extend the OTP requirement to other online banking activity including login. He said he wanted to continue to access and use online banking without needing to have a mobile phone. He asked if Santander would send spoken OTPs to a landline phone number instead.

At that stage Santander were requiring OTPs for some payments to existing payees, and for all payments to new payees, and the complaints handler was unaware of any plans to extend OTPs to the login process. They didn't uphold Mr B's complaint. They explained they wouldn't use landlines to authenticate payments because that's "*less secure*" than mobile phones.

In July 2019 Santander let their customers know that they'd be making some changes, and that to access online banking they'd either need their mobile banking app or to receive an OTP to a mobile phone. They said the changes were "*driven by new banking regulation designed to further protect* [customers] *from fraud*". Mr B complained again asking Santander to rethink this change as it would prevent him from accessing online banking at all.

Santander said customers without mobile phones could continue to bank using branch and telephone banking services. They added that customers with poor mobile phone reception but with a tablet device would be able to authenticate using the app. They confirmed other options would continue to be explored but they couldn't provide Mr B, a customer without a mobile phone and wanting to access online banking via a PC, with a solution at that time.

Mr B disagreed that receiving an OTP to a mobile phone is a secure way of authenticating and cited reports of OTP messages being intercepted by fraudsters. He also highlighted that other payment service providers (PSPs) offer customers without mobile phones the option of authenticating using their landline phone number or provide card readers, secure keys or authentication apps.

When Mr B brought his complaint to this service, he said Santander had used the regulations as a "*bogus excuse*" for "*downgrading*" the experience of customers without mobile phones. He described branch and telephone banking services as "*plainly inferior*

options" to online banking and told us he wants Santander to offer authentication options for online banking that don't rely on mobile phones.

Santander told us they'd added two-factor or strong customer authentication (SCA) to the process for customers accessing their online banking in compliance with EU regulations. They added that the need for customers to have a mobile phone to access the full range of Santander's services is part of their terms and conditions and has been since 2014.

Our investigator's view

Our investigator upheld Mr B's complaint. Whilst she didn't think Santander had acted unfairly by introducing SCA – an important regulatory measure designed to protect both Santander and customers from fraud – she said Santander should've come up with authentication methods that don't rely on mobile phones. She said branch and telephone banking are alternatives to online banking, not alternatives to authenticating customers who want to use online banking or make online payments. So, she didn't think Santander had acted fairly.

Taking into account that at the time of her view (December 2020) Mr B was still able to login to his online banking without an OTP, our investigator sought to compensate Mr B for the distress and inconvenience he'd been caused by; the prospect of losing access to his online account, and how Santander had communicated the SCA changes to him. She said Santander should pay Mr B £150 and offer him a viable alternative to authenticating that doesn't rely on a mobile phone.

Responses to the view

Santander agreed to pay Mr B £150. They also offered to send Mr B an OTP to an email address for him to use to login to online banking, and offered to add an exemption to prevent interruption when he uses his card for online shopping. They said this would be until they can offer an alternative authentication option that he has access to.

However, Santander said they wouldn't change the SCA process for online payments to new payees or for payments to existing payees which hit a fraud prevention rule. For those transactions, they said Mr B would still need to authenticate by receiving an OTP to mobile phone or make the payment using telephone (an OTP support line) or branch banking.

Santander pointed out that for these transactions there had been no change in their process; the ability to set up new payees without a mobile phone was not a service that had ever been available to Mr B. They said customers had been required to authenticate payments to new payees with an OTP to mobile phone since at least 2014.

Mr B accepted the £150 compensation, but he wasn't completely happy with Santander's offer. He said the solution of email OTPs was acceptable to him along with the suggested exemption for online shopping. He also acknowledged that when he needs to authenticate a large payment or set up a new payee, telephone banking "*provides a remedy*" and causes only "*minor inconvenience*". But he was dissatisfied that Santander's offer maintained a "*two tier system*" and continued to "*discriminate against those without a mobile phone or adequate reception*". Overall, he didn't think Santander's solution went far enough.

As no agreement could be reached, the complaint was passed to me to decide.

A further response from Santander – February 2022

While I've been reviewing Mr B's complaint our service has kept talking with Santander about their approach to SCA for customers who don't have or can't use mobile phones to authenticate. Following these discussions, which have focussed on complaints with similar features to Mr B's rather than Mr B's complaint specifically, Santander's approach to SCA has evolved further. Santander have let me know that they are in the process of developing an OTP via email ('email OTP') solution for customers who are unable to use a mobile phone or who don't have one. This method of strong customer authentication will be available for Mr B to use when he wants to set up a new payee in online banking.

My provisional decision

I issued a provisional decision on 3 March 2022. I began by setting out the considerations I thought relevant to my decision. I wrote:

> "*I'm required to determine this complaint by reference to what I consider to be fair and reasonable in all the circumstances of the case. When considering what is fair and reasonable, I am required to take into account: relevant law and regulations; regulators' rules, guidance and standards; codes of practice; and, where appropriate, what I consider to have been good industry practice at the relevant time.*
>
> *So, I'll start by setting out what I've identified as the relevant considerations to deciding what is fair and reasonable in this case.*
>
> *The terms and conditions of Mr B's account*
>
> *From 2014 to 12 January 2018 the terms and conditions relevant to Mr B's account explained:*
>
> > *"11.1.1 The One Time Passcode is an added security function integral to Your use of the Services. For the One Time Passcode to operate You must have registered Your mobile phone number with Us in respect of Your Account(s). The registered mobile phone must be able to receive calls and text messages.*
> >
> > *11.1.2 If You do not register a mobile phone number with Us, Your access to the Online Banking Service may be limited; for instance, You will not be able to set up new payees."*
>
> *The terms and conditions changed on 13 January 2018. The change relevant to this complaint read as follows:*
>
> > *"7.1 To login to your account, make payments and access many aspects of the services you will need to register your mobile phone number to receive one-time passcodes that we will send to your phone. You will need to input this code to verify and complete certain transactions."*
>
> *The Payment Services Regulations 2017*
>
> *The Payment Services Regulations 2017 (the PSRs) Reg. 100, which came into force on 14 September 2019, says that a payment service provider (PSP) must apply "strong customer authentication" where a "payment service user" accesses its payment account online, initiates an electronic payment transaction; or carries out any action through a remote channel which may imply a risk of payment fraud or other abuses.*

Strong customer authentication (SCA) is defined in the PSRs. It means:

> *"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");"*

The Financial Conduct Authority (FCA) and UK Finance have both issued guidance to PSPs on the implementation of SCA. The FCA in its guidance document "Payment Services and Electronic Money – Our Approach" says:

> *"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 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****." (my emphasis)*

Later in the document the FCA explains that whilst PSPs may choose not to apply SCA where a payer initiates a payment to a trusted beneficiary, "Strong customer authentication is required when a payer requests its PSP to create or amend a list of trusted beneficiaries".

UK Finance has also issued guidance to businesses detailing a non-exhaustive list of authentication methods a PSP can employ to satisfy the "possession" element of SCA. These include:

- *Possession of a device evidenced by an OTP generated by, or received on a device (such as OTP by SMS text message)*
- *Possession of a device evidenced by a signature generated by a device (hardware or software)*
- *App or browser with possession evidenced by device binding*
- *Card or device evidenced by QR code scanned from an external device*
- *Possession of card evidenced by a card reader*
- *Possession of card evidence by a dynamic card security code*
- *OTP received by email account associated, bound or linked adequately to the cardholder*
- *OTP received by landline number associated, bound or linked adequately to the cardholder*

What I've provisionally 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 done so, I'm minded to agree with the investigator and uphold Mr B's complaint.

As I've set out above, PSPs like Santander were required under the PSRs 2017 to implement SCA. The timeline for this has been subject to change because of the Covid-19 pandemic. But ultimately PSPs had until March 2020 to implement SCA for online banking, and the FCA has given the e-commerce industry until March 2022 to implement SCA for online payments.

In response to this regulatory requirement Santander reinforced some of their existing processes to which OTPs to mobile phone were already "integral", such as the process for setting up new payees. They also extended the need to receive an OTP to mobile phone to the online banking log in process. It was these changes that prompted Mr B's complaint because he doesn't own a mobile phone or another mobile device, and without these he was concerned that his experience of Santander's online banking and payment services would be downgraded. Mr B didn't think this prospect was fair to him, or to people without mobile phones more generally.

I think it's important to note that Mr B doesn't disagree with SCA in principle. But he doesn't think he should have to have a mobile phone to complete SCA or, without one, be left with the less easy and less convenient options of telephone and branch banking. In short, his only complaint is about Santander's decision to send the OTPs he needs to strongly authenticate him to mobile phones only. I should point out that Santander do offer customers the ability to strongly authenticate using their mobile banking app, but as Mr B doesn't have any mobile device at all that's not a viable option for him either.

It's also important to say that I don't think Santander acted unfairly by implementing SCA. I'm satisfied that the regulations and guidance I've cited above mean that Santander were obliged to implement two-factor authentication or SCA to the online account login process, and also to electronic payments and some other remote banking actions. Fraud associated with online banking and electronic payments is a significant risk to both businesses and consumers, and the SCA measures are intended to enhance the security of payments, reducing that risk.

But when they implemented SCA I think Santander should have taken into account that there are, and will continue to be, customers who, for a variety of reasons, can't rely on possession of a mobile phone or device to authenticate themselves. And Santander should've taken steps to manage the potential negative impact of SCA on these customers. The FCA's guidance on this subject has been clear; PSPs such as Santander "must" provide viable methods for customers who don't possess a mobile phone or are in areas without reliable mobile phone reception to strongly authenticate. I don't think the FCA is saying this only applies to customers who can't rely on mobile devices for a specific reason (such as age, disability or vulnerability). I think the guidance is aimed at making sure online banking and electronic payment services are inclusive of non-mobile phone users, regardless of the reason why they don't have or use a mobile phone.

That's not to say that sending OTPs to mobile phones is an unreasonable method of strongly authenticating customers. I recognise it's a method that will be viable for many, and there's nothing wrong in my view with Santander choosing it as their primary method of strongly authenticating customers using their online banking and electronic payment services. However, when Mr B complained that this wasn't a

viable method for strongly authenticating him, I think Santander should have offered him alternatives.

As I've indicated above in my summary of what's happened, Santander are now offering Mr B viable alternatives. He can now receive email OTPs for accessing his online banking; Santander will soon be sending email OTPs for strongly authenticating online card payments and setting up new payees; and they've adopted a permitted exemption from SCA for electronic payments to trusted beneficiaries.

In light of Santander's most recent offer (to send email OTPs for strongly authenticating new payees) I think there will now be very few, if any, instances where Mr B will find he can't receive an OTP and has to do something else (such as call Santander) to verify an activity he's trying to complete online. My understanding is that he still might have to do this if an activity has hit a fraud prevention rule. And I don't think Santander's offer of email OTPs currently extends to occasional and risky remote activities such as updating contact details (I'd like to invite Santander to confirm or correct my understanding in response to this provisional decision). This means that there are still likely to be residual differences in experience for customers like Mr B who don't own a mobile phone/device. But there are two things I think I should say about that.

Firstly, if, following Santander's implementation of their email OTP solution, Mr B can do everything bar very occasional and specific activities such as updating his contact details without a mobile phone, I think he's likely to only experience infrequent and minor inconvenience.

Secondly, Santander have repeatedly told us that they wouldn't extend the use of email OTPs further or introduce another non-mobile phone-based authentication method for all online activities because it's not within their risk appetite. I appreciate this and don't underestimate the risks which the growth of online payments presents, but I also note UK Finance have set out a range of methods a PSP can use to satisfy the "possession" element of SCA, so I don't think OTP to mobile phone is the only feasible way to mitigate the fraud risk. That said, I accept that businesses may use different systems and that Santander are telling me there are limitations to what they can offer. They'll send email OTPs for logging on to online banking, making online card payments and, soon, setting up new payees, but not, it seems, for all actions a payment service user might carry out remotely. Some activities might still need an OTP to mobile phone and in the absence of being able to receive one, a phone call to Santander's OTP support line. I also accept that I cannot require Santander to offer Mr B an option that it currently doesn't offer, and I don't have evidence to support that it'd be practical or possible for Santander to do so. Therefore, the only remedy I believe will adequately address this issue is compensation.

I think the SCA alternatives Santander are now offering do resolve the complaint Mr B brought to us. But I think it's important to note that before their most recent offer to extend email OTPs to the process for setting up new payees, I was minded to agree with Mr B and our investigator that Santander's approach to SCA wasn't in line with what's expected by the regulator or industry bodies. I don't think leaving Mr B unable to use the full range of online banking and electronic payment services offered by Santander, and reliant on telephone banking (the OTP support line) was a fair and reasonable thing to do. In short, I think Santander's approach put Mr B at an unfair disadvantage because he doesn't have a mobile phone.

Until recently Santander's position was that they were offering a viable alternative for strongly authenticating the creation of new payees – their OTP support line or

telephone banking. But I don't agree that a telephone line, dedicated or otherwise, is a satisfactory alternative for strongly authenticating.

In my view, if Mr B must call a telephone number and speak with a Santander agent whenever he needs to create a new payee or amend one, he's no longer strongly authenticating. Indeed, he's using a banking channel (telephone banking) for which SCA isn't normally required. So, I don't think the OTP support line can reasonably be interpreted as an alternative way of strongly authenticating. Put simply, I think it avoids the SCA requirements altogether and is an alternative way of banking; an alternative way of banking which is less convenient, more time consuming and more restrictive, than online banking.

If Mr B has to call a telephone number whenever he wants to create a new payee the process would be subject to the usual telephone banking communications which means he would need to wait for his call to be picked up. He'd then have to go through telephone banking security, explain the reason for his call and go through the process of creating the new payee before he'd be able to make a payment to that payee. It's a process that would take time, in all likelihood longer than the time it would take if all Mr B had to do was enter the new payee's details into an online banking screen and receive an OTP to authenticate the change. I think this is a very different level of service to that afforded to customers with mobile phones. Taking all of this into consideration, I don't think the OTP support line was a fair and reasonable solution to Mr B's complaint.

Santander have indicated to this service that part of their rationale for not offering another alternative for strongly authenticating the creation of new payees before now, was that their customers have needed to receive an OTP to mobile phone to carry out this activity electronically for some years. They've pointed to their online banking terms and conditions from 2014 onwards as evidence of this. I've thought carefully about this point, but I'm not persuaded it makes a difference to my finding that Santander should be offering Mr B a viable alternative so that he can strongly authenticate when carrying out this activity too.

Under the PSRs 2017 PSPs are required to apply SCA, amongst other occasions, when a payment service user carries out any action through a remote channel which may imply a risk of payment fraud or other abuses. This means SCA is required when a payment service user requests its PSP to create or amend a list of trusted beneficiaries. As SCA is required by regulation to be applied to this activity, I think the FCA guidance which says PSPs should provide different methods of authentication, and "must" provide a viable means to strongly authenticate payment service users without mobile phones, also applies. I don't think this is guidance that Santander can disregard on the basis that they were only offering OTP to mobile for setting up new payees previously. The fact is there's been FCA guidance since the inception of SCA which says that's not enough. Offering only one mobile phone-based method of strongly authenticating any activity to which SCA applies, excludes non-mobile phone users from that activity. I don't think that's right when there are other non-mobile phone-based options for SCA that PSPs can employ which are more inclusive.

I agree with and provisionally uphold Mr B's complaint about Santander's approach to SCA. I provisionally find that it's not fair or reasonable of Santander to exclude Mr B from some of their online banking and electronic payment services, just because he doesn't possess a mobile phone. Treating Mr B fairly in my opinion involves making it possible for him to strongly authenticate so that he can fully use

Santander's online banking and electronic payment services and doesn't have to rely on telephone and branch banking services instead.

In short, I think he should be able to access his online banking from a computer, make online payments to trusted and new payees, verify electronic payments, shop using his debit card online, and perform similar actions online, with a level of ease and convenience equal to that of mobile device users.

Santander have now offered to send email OTPs for most online banking and payment activities requiring SCA. I think this offer will broadly level the online banking and payment experience of Mr B with Santander's mobile device using customers. As I've noted already, I think Santander's offer does leave a residual difference in that there will be some remote and risky activities such as updating contact details for which I don't think Mr B will be able to receive an OTP and so will have to call up or visit a branch. But I think this is likely to cause Mr B only infrequent and minor inconvenience at most. And I can't direct Santander to extend the email OTP offering to more activities when Santander are telling me that it's not something they're prepared or able to do, and I have no evidence it'd be practical or possible for them to do so.

Santander's offer to send Mr B an OTP to an email address for him to use to login to online banking; to add an exemption to prevent interruption when he uses his card for online shopping (until they can offer an alternative authentication option that he has access to); and to send him email OTPs for the purpose of setting up new payees is, I think, fair and reasonable. However, I think it's important to recognise that it's taken a significant length of time to reach this position, time during which Mr B's access to online banking and payment services has been affected by the fact that he doesn't have a mobile device. And I think this needs to be reflected in the award I make for distress and inconvenience.

In deciding whether or not to award compensation, and if so, how much, I'm satisfied that in this case I have to take into account the impact Santander's actions have had to date. As I've said above, I think the current position (which I've asked Santander to confirm) does leave some residual unfair differences between the online banking experience of mobile phone users and customers like Mr B who don't have a mobile phone. But I don't think it would be appropriate to award compensation for the impact these differences might have on Mr B in the future, even though they may do so. I say this because Santander might decide to change its approach, or the issue may not arise again. I want to be clear that this decision addresses matters from the date Mr B complained (mid-2019) to the date of this decision only. It may be that the issue arises again – when Mr B tries to undertake an online activity which he finds requires him to receive an OTP to a mobile phone – and if the matter cannot be resolved, it may result in a new complaint.

Our investigator said Santander should pay Mr B £150 compensation. This amount appeared fair due to the possibility of other options being put in place within a reasonable timeframe, and the expectation that the inconvenience would lessen with those other options. But as Santander have only just agreed to develop the email OTP solution for the setting up of new payees – more than a year since our investigator issued their view (December 2020) – and as there is currently no set date for when the solution will be implemented, I've considered the award again. I consider a higher award would better address the issue and reflects the increased distress and inconvenience caused to date. In the circumstances, I think an award of £350 would be more appropriate.

For the reasons I've explained I intend to uphold Mr B's complaint. Santander have already agreed to make some changes to how they strongly authenticate Mr B and I think their offer is fair in all the circumstances.

So, my provisional decision is that Santander UK Plc should:

- *Send Mr B OTPs to his email address for him to use to login to online banking;*
- *Add an exemption allowing him to use his card for online shopping without a mobile phone, until they can offer an alternative authentication option that he has access to; and*
- *Send Mr B OTPs to his email address for him to use when he wants to set up a new payee.*

Additionally, Santander should:

- *Pay Mr B £350 compensation for the distress and inconvenience caused by: the way Santander communicated the SCA changes to Mr B; the disruption he's experienced to his online banking and payment services since Santander implemented SCA; and the length of time it's taken Santander to offer a viable authentication solution*."

Responses to the provisional decision

Santander confirmed they'd arrange for Mr B to receive email OTPs so that he can set up new payees (and amend existing payees) in online banking. They also let us know that they plan to deploy the enhanced email OTP solution in June 2022, subject to testing and development.

Mr B made the following comments:

- He accepted the provisional decision I'd reached, and was happy with my provisional direction for how Santander should put things right.

- He wanted it noted that he'd not raised a complaint about needing to register a mobile phone earlier, for example when Santander's Terms and Conditions changed in January 2018, because he'd not been alerted to the issue until he read a press article in February 2019. He said:

  "*Much of the distress and inconvenience caused to me these past three years has been due to what I consider to be Santander's abject failure to communicate effectively with me (and within the business, for that matter). Repeatedly, I have not been informed of planned or actual changes that would affect my customer experience*."

- He said his recent experience of telephone banking has been poor; underlining the fact that telephone banking is not a satisfactory alternative to online banking.

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.

As neither party provided any further evidence or arguments to counter what I said in my

provisional decision, I see no reason to depart from the provisional conclusions I reached.

For all the reasons set out in my provisional decision, I find that Santander treated Mr B unfairly when they didn't offer him a viable alternative to strongly authenticating with a mobile phone. So, I uphold his complaint.

Putting things right

As I set out in my provisional decision, to put things right Santander UK Plc should, as they've already offered to do:

- Send Mr B OTPs to his email address for him to use to login to online banking;
- Add an exemption allowing him to use his card for online shopping without a mobile phone, until they can offer an alternative authentication option that he has access to; and
- Send Mr B OTPs to his email address for him to use when he wants to set up a new payee (or amend an existing one).

Santander should also:

- Pay Mr B £350 compensation for the distress and inconvenience caused by: the way Santander communicated the SCA changes to Mr B; the disruption he's experienced to his online banking and payment services since Santander implemented SCA; and the length of time it's taken Santander to offer a viable authentication solution.

If Mr B accepts this decision, my expectation is that Santander should pay him the £350 within 28 days of his acceptance.

With regard to the changes they've agreed to make so that Mr B can strongly authenticate without a mobile phone, I expect Santander to make those changes which they haven't already, as soon as possible. If Santander's plan to implement email OTP for new payees is not completed by June 2022 as they've indicated, I'd expect Santander to keep Mr B informed and to consider the impact of any further delay on him.

My final decision

It's my final decision to uphold Mr B's complaint. Santander UK Plc should take the actions I've set out in the 'Putting things right' section of this decision.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 22 April 2022.

Beth Wilcox
Ombudsman