DRN-3362545

The complaint

Mrs R complains that because she doesn't have a mobile phone, she's not able to fully access and operate her Santander UK Plc bank accounts online. As one of those accounts is held jointly with Mr R, we've obtained his consent to us looking into this complaint, but I'll refer to Mrs R throughout as it's her online banking and electronic payments service the complaint is about.

What happened

In early 2020 Mrs R logged into online banking and tried to add a new payee to make an electronic payment to. When she submitted the new payee's details the system told her a one-time passcode (OTP) had been sent to her old mobile phone number to authenticate the change. As Mrs R no longer owned a mobile phone, she contacted Santander to remove the number and replace it with her landline. Santander told her they couldn't remove the mobile phone number from her account without replacing it with another.

Mrs R complained. She was concerned she needed a mobile phone to complete payments through online banking, and that an OTP had gone to a mobile phone number she no longer owned.

Santander firstly sought to reassure Mrs R that the OTP which had been sent to her old mobile phone number wasn't a risk to her account. They then explained OTPs were part of their "*new security process*" and had been implemented in response to an EU Directive to ensure "*account safety*". They said she could still manage her account without a mobile phone through telephone or branch banking. They also confirmed they couldn't amend the mobile phone number linked to her account unless she replaced it with a new one. Santander did offer to register an email address on the account to receive OTPs, but said these would have limited application.

When Mrs R brought her complaint to this service, she said she has no objection to authentication by OTP and agrees that online security is of vital importance. But she objects to being told she must have a mobile phone in order to operate her accounts fully. She said:

> "*I feel I am being disadvantaged and discriminated against because I do not have a mobile phone … The outcome I am hoping for is to be able to operate my Santander accounts, without a mobile phone, as easily and efficiently as anyone else*."

What Santander told us

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 said where customers have no SMS text message facility (mobile phone) they can now send OTPs to email for the online banking log in stage, but this would not apply to any other transactions within online banking (such as setting up new payees). Santander showed us that Mrs R had been registered for email OTPs in July 2020.

Mrs R's thoughts on email OTPs

Our investigator spoke with Mrs R about whether email OTPs had resolved her complaint. Mrs R said this didn't provide a complete solution because, although she could now log in to online banking without a mobile phone, she was still unable to set up new payees online or make other changes on her account. Mrs R told us that having to call to set up a new payee negates the "*ease and convenience of online banking*".

Our investigator's view

Our investigator upheld Mrs R's complaint. Whilst he didn't think Santander had acted unfairly by introducing SCA – an important regulatory measure designed to protect both Santander and customers from fraud – he said Santander should've come up with authentication methods that don't rely on mobile phones. Particularly as the Financial Conduct Authority (FCA) had been clear that businesses should provide authentication methods that do not rely on mobile phones to cater for consumers who will not have or won't want to use a mobile phone.

He said branch and telephone banking are alternatives to online banking, not alternatives to strongly authenticating customers who want to use online banking or make online payments. So, he didn't think Santander had acted fairly. He also said it was unreasonable of Santander not to remove Mrs R's old mobile phone number when she'd asked.

To put things right he said Santander should pay Mrs R £150 compensation to reflect the trouble she's had adding new payees to her account, and the concern she was caused by OTPs being sent to an old mobile phone number. He also said Santander should develop strong customer authentication solutions that don't rely on mobile phones, and remove her old mobile number from her account.

Responses to the view

Mrs R accepted this outcome but added to her complaint that it had now become necessary to receive an OTP to mobile phone when using her debit card online. She said she'd recently had to abandon an online card payment because she has no mobile phone to receive OTPs to.

Santander removed Mrs R's old mobile number from her account. They also offered to add an exemption to prevent interruption when she uses her debit card for online shopping. They said this would be until they could offer an alternative authentication option that she has access to.

However, Santander didn't agree to pay the £150 compensation recommended by the investigator and said they wouldn't change their process for online payments to new payees or for online payments to existing payees which hit a fraud prevention rule. For those transactions, they said Mrs R would still need to authenticate by receiving an OTP to mobile phone or make the payment using telephone or branch banking. They explained they have a dedicated OTP support line via which Mrs R can set up a new payee (a "*trusted beneficiary*") and then continue her online banking journey. So, they said, Mrs R had a viable alternative to using a mobile phone for authentication. They also said setting up new payees should only be a small part of Mrs R's interaction with online banking.

Santander also told us that for these transactions there'd been no change in their process; the ability to set up new payees online without a mobile phone was not a service that had been available before their implementation of SCA. They said customers had been required to authenticate payments to new payees with an OTP to mobile phone since at least 2014.

Mrs R didn't think Santander's response went far enough or resolved her complaint because she still couldn't operate her account fully online without a mobile phone. She said it's not just the setting up of new payees she can't do online without a mobile phone. She's also found she can't make changes to her personal or contact details without receiving an OTP to a mobile phone.

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

A further response from Santander – February 2022

While I was reviewing Mrs R's complaint our service 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 focussed on complaints with similar features to Mrs R's rather than Mrs R's complaint specifically, Santander's approach to SCA evolved further. Santander let us 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 Mrs R to use when she wants to set up a new payee in online banking.

My provisional decision

I issued a provisional decision on 25 February 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.*
>
> *Santander's online banking terms and conditions*
>
> *From 2014 to 12 January 2018 Santander's online banking terms and conditions included the following:*
>
> > *"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****." (my emphasis)*
>
> *These 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 onetime passcodes*** *that we will send to your phone. You will need to input this code to verify and complete certain transactions." (my emphasis)*

The Payment Services Regulations 2017

The Payment Services Regulations 2017 (the PSRs) implemented an EU Directive from 2015 commonly known as the revised Payment Services Directive, or PSD2.

Reg. 100 of the PSRs 2017 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. The FCA has said that telephone banking is out of scope of Reg. 100, although PSPs can extend strong customer authentication to this channel on a voluntary basis. So, SCA is something PSPs have to apply to online banking and card payments, and activities such as creating or amending payment mandates online.

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");"*

As a minimum, the elements or factors used in SCA must derive from two of the three above categories.

The 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" (June 2019) 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 Mrs R's complaint. I'll explain why.

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 Mrs R's complaint, because she doesn't own a mobile phone or another mobile device, and without these she found she was, firstly, unable to make payments to new payees through online banking and, shortly afterwards, faced with being unable to even log in to online banking without a mobile phone. More recently, she's also been prevented from using her Santander debit card to make online payments because she can't receive OTPs via SMS text message. Mrs R doesn't think this is fair to her, or to people without mobile phones more generally.

I think it's important to note that Mrs R doesn't disagree with SCA in principle. She's explicitly said she acknowledges the importance of online banking and payment security. But she doesn't think she 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, her only complaint is about Santander's decision to send the OTPs she needs to strongly authenticate her 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 Mrs R doesn't have any mobile device at all that's not a viable option for her either.

Since receiving Mrs R's complaint in April 2020 Santander's approach to SCA has evolved. They're now sending OTPs to Mrs R's email address so that she can log in to online banking and carry out some online banking activities (for example, view her account balances and statements and make payments to trusted beneficiaries). They're also prepared to add an exemption allowing her to use her card for online shopping without a mobile phone; and have very recently told us that they'll be

extending the use of email OTPs to online card payments and, shortly, the process for setting up new payees.

I'm pleased to note these developments because Santander's approach to SCA until very recently left Mrs R unable to use the full range of online banking and electronic payment services offered by Santander, and reliant on telephone banking (or their OTP support line). I don't think that was fair and reasonable and I don't think Santander's approach to SCA was in line with what's expected by the regulator or industry bodies. And, importantly, I think Santander's approach put Mrs R at an unfair disadvantage because she doesn't have a mobile phone.

In my view, if Mrs R had to call a telephone number and speak with a Santander agent whenever she needed to create a new payee, she'd no longer be strongly authenticating. Indeed, she'd be 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 Mrs R has explained she finds less convenient, more time consuming and more restrictive, than online banking.

If Mrs R had to call a telephone number whenever she wanted to create a new payee the process would be subject to the usual telephone banking communications which means she would need to wait for her call to be picked up. She'd then have to go through telephone banking security, explain the reason for her call and go through the process of creating the new payee before she'd be able to make a payment to that payee. It's a process that would take time; longer than the time it would take if Mrs R could 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.

So, I think it's right that Santander are now going to be offering email OTP for the process of setting up new payees. But it's disappointing this offer has been so long coming (almost two years since Mrs R made her complaint), and in the interim Mrs R's online banking and payment activity has been limited by the fact she doesn't have a mobile phone.

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. So, I don't think Santander acted unfairly by implementing SCA.

But when doing so, I think Santander should've 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 Mrs R complained that this wasn't a viable method for strongly authenticating her, I think Santander should have offered her alternatives.

Santander are now offering Mrs R viable alternatives. She can now receive email OTPs for accessing her 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. So, my understanding is that the only time she's likely to need to call Santander will be to verify any activity that has hit a fraud prevention rule – the need for this is, I think, likely to be infrequent.

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, is 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've offered Mrs R a viable alternative when she first complained so that she could 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 could 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 which says that's not enough since the inception of SCA. 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 note that Santander haven't said they'll be extending the email OTP solution to any and all online activity for which an OTP is currently required. This means that when Mrs R wants to make changes to her personal or contact details she might still not be able to do that without receiving an OTP to a mobile phone. Mobile phone OTPs might also be required when any other online activity hits a fraud prevention rule. If that's the case (and I invite Santander to confirm whether it is in response to this provisional decision), then there will remain some residual differences between the online banking experience of mobile phone users and customers like Mrs R who don't have a mobile phone. I'm not satisfied that's fair. As I've said, offering only one mobile phone-based method of strongly authenticating any activity to which SCA

applies, excludes non-mobile phone users from that activity. But there are two things I'd say about this.

Firstly, if, following Santander's implementation of their email OTP solution, Mrs R can do everything bar very occasional and specific activities such as updating her contact details without a mobile phone, I think she'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 to which SCA applies. 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 Mrs R 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.

Putting things right

I agree with Mrs R's complaint and I provisionally find that it's not fair or reasonable of Santander to exclude Mrs R from some of their online banking and electronic payment services, just because she doesn't possess a mobile phone. Treating Mrs R fairly in my opinion involves making it possible for her to strongly authenticate so that she 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 she should be able to access her online banking from a computer, make online payments to trusted and new payees, update her details, verify electronic payments, shop using her card online, and perform similar actions online, with a level of ease and convenience equal to that of mobile device users.

Santander have changed their approach to SCA since Mrs R first complained in April 2020. Mrs R will, once Santander have implemented their recently offered email OTP solution, be able to make online card payments, access her online banking and make electronic payments to trusted beneficiaries and new payees unimpeded by not having a mobile phone. So, to put things right here I'm going to say that Santander UK Plc should, as they've already offered to do:

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

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 Mrs R who don't have a mobile phone. But I don't think it would be appropriate to award compensation for the impact these differences are likely to have on Mrs R 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 Mrs R complained (April 2020) to the date of this decision only. It may be that the issue arises again – when Mrs R tries to undertake an online activity which she finds requires her 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 Mrs R £150 compensation to reflect the distress and inconvenience caused by not being able to do certain online banking and payment activities without a mobile phone. 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 – almost a year since our investigator issued their view – 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."

Responses to the provisional decision

Santander agreed to do what I'd said in my provisional decision. They also let us know that they plan to deploy the enhanced email OTP solution in June 2022 subject to testing and development.

Mrs R made the following comments in response to the provisional decision:

- When she's tried to make payments to existing payees but changed the payment reference details, that's necessitated receiving an OTP to a mobile phone too – Santander's system treats amendments to existing payees as if they're new payees and this has had a "*significant impact*" on her ability to operate her account.

- Whilst she's happy Santander have added an exemption allowing her to use her card for online shopping without a mobile phone, she's concerned this doesn't offer the same high level of security that mobile phone users enjoy, and she wants an equally secure alternative authentication option that she can access as soon as possible.

- Santander's agreement to develop the email OTP solution for use when setting up new payees is "*welcome*", but until it's implemented she will continue to suffer "*inconvenience, distress and discrimination*" and the £350 only compensates her for the distress and inconvenience caused until the date of the decision.

- She's concerned that I cannot require Santander to offer an authentication 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*" – she thought I should be able to "*insist that Santander change their operating practices or systems*".

- Santander's recent customer information communications show that they continue to focus on mobile phone OTPs, "*They make no mention of the current exemption option they have offered me, as a non-mobile user, for this activity. It seems they have no interest at all in communicating with customers who do not use a mobile phone …*"

Mrs R also said:

> "*I find it hard to accept that Santander cannot find workable alternatives (many other banks and even HMRC have successfully adopted alternative solutions), and even harder to believe that their refusal to do so can go unchallenged …* [I] *am pleased that the ombudsman has decided to uphold* [my complaint]*, and also recommended that some compensation payment from Santander is appropriate.*
>
> *I am, however, extremely disappointed that more robust action has not been taken against Santander to 'put the matter right'. I am also dismayed that Santander can continue to discriminate against non-mobile users, in contravention of the Regulations and all official guidance*."

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 done so, I see no reason to depart from the provisional decision I reached – I uphold Mrs R's complaint. Santander should make the changes they've now agreed to make so that Mrs R can access her online banking, make online card payments, and make electronic payments to trusted beneficiaries and new payees without reliance on a mobile phone.

I appreciate that Mrs R has felt discriminated against by Santander because she doesn't use a mobile phone – she's told me they've made her feel like a "*second class customer*" – and I agree with her that this should not have happened. I think I set out clearly in my provisional decision that I don't think Santander's treatment of Mrs R has been fair or reasonable, and I don't think Santander's approach to SCA has been in line with what's expected by the regulator or industry bodies. My view on that hasn't changed.

Mrs R doesn't feel that Santander's approach to SCA has been sufficiently challenged. But through upholding Mrs R's and similar complaints, I think Santander's approach has been challenged, and it's through that process that their approach to SCA has evolved. Mrs R is also disappointed that my direction to Santander to put things right isn't more robust, because, as I acknowledged in my provisional decision, even Santander's evolved approach doesn't result in complete parity of experience between mobile phone users and those customers who don't have or can't use mobile phones to authenticate.

But it's not our role to dictate what SCA methods Santander should offer, and any direction I give must be clear and practical for the business to implement. And in the circumstances that Santander are telling me they're unable, due to risk and system considerations, to extend the use of email OTPs further, I can't give a direction that they should do so without evidence to support that it'd be practical or possible.

Our role is to consider whether financial businesses, in this case Santander, have acted fairly and reasonably in the circumstances of an *individual* complaint. Where they haven't, we consider the consequences of what they've done and try to put the individual complainant back in the position they would otherwise have been in. That's what we mean by putting things right. Broader changes to the way a business operates would be for the

industry regulator (the FCA) to pursue. Whilst the FCA doesn't investigate individuals' complaints against the firms it regulates, we share the insight from the complaints we see so that the FCA can use that insight to inform the regulatory and enforcement action it takes.

It is the case that Mrs R may still have to call Santander's telephone banking service more frequently than a customer who is able to receive OTPs to a mobile phone or use the mobile banking app. But with Santander's agreement to send email OTPs for strongly authenticating all of the main online banking and payment activities, the occasions on which Mrs R's experience differs from that of a mobile phone user should be infrequent and cause no more than minor inconvenience. And if that's not the case, if Mrs R's ability to undertake an online banking or payment activity related to her Santander accounts is frustrated because she can't receive an OTP to a mobile phone, and if the matter cannot be resolved, it may result in a new complaint.

The evolved position is that Santander now offer email OTPs for those customers who can't rely on possession of a mobile phone or device to authenticate themselves. Santander have told me that for setting up new payees (which includes amending existing payees) email OTPs are expected to be available in June 2022. So, Mrs R should soon be able to operate her account online very much like a mobile phone user would. I think that, along with the compensation I've recommended, results in a fair and reasonable outcome here.

Mrs R has pointed out the £350 I've recommended only compensates her for the inconvenience she's experienced to date, but says her "*inconvenience, distress and discrimination*" will continue until Santander implement the enhanced email OTP solution. I appreciate the point Mrs R is making here but I don't think it would be appropriate to increase the award I've made further. Our awards for distress and inconvenience are made in the round rather than calculated on the exact number of days, weeks or months a consumer has been inconvenienced. Whilst I understand that Mrs R will continue to have to rely on telephone banking for setting up new payees and amending existing ones for another few months (until approximately June 2022), she will be able to log in to online banking, pay existing payees (without amendments) and make online card payments, all without having a mobile phone. So, her inconvenience will be limited. I'm also mindful that although I think Santander should have made these changes earlier, now they've agreed to do so, they do need a reasonable period in which to implement them. So, I won't be asking Santander to pay Mrs R more than £350. Of course, if Santander do not implement the enhanced email OTP solution in accordance with their planned timescale, I'd expect them to give consideration to how any delay would further impact Mrs R.

Turning to Mrs R's concern that the current exemption applied to her card for online card payments doesn't offer the same high level of security that mobile phone users enjoy, and her request to have an equally secure alternative authentication option that she can access as soon as possible, Santander have confirmed that they are planning to roll out email OTPs for authenticating online card payments also. Although Santander haven't provided a timescale for that part of their plan I hope Mrs R will be reassured to know that, in the meantime, she should be able to make online card payments without interruption (unless the activity has hit a fraud prevention rule) and, importantly, that nothing about the exemption Santander has applied to her card changes Mrs R's liability for unauthorised transactions. So, if Mrs R's card details are used to make unauthorised payment transactions online there are still only very limited circumstances in which she wouldn't be entitled to a refund.

With regard to Mrs R's comment that Santander's recent customer information communications show that they continue to focus on mobile phone OTPs, I appreciate that this generates Mrs R's ire in the context that she has no interest in having a mobile phone and has been fighting to be given an alternative method to strongly authenticate since at least early 2020. But as I've said before, I see nothing wrong in Santander choosing mobile

phone OTPs as their primary method of strongly authenticating customers. I also see no error in Santander encouraging customers to register their current mobile phone number or use the mobile banking app so that they can securely authenticate. The important thing is that when a customer tells Santander that they don't have a mobile phone or can't use the app, Santander offer a viable alternative.

Overall, I'm upholding Mrs R's complaint. I don't think Santander's implementation of SCA treated Mrs R fairly and reasonably as they didn't offer her, someone who doesn't have a mobile phone, a viable alternative for strongly authenticating when they should have done.

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 Mrs R OTPs to her email address for her to use to login to online banking;
- Add an exemption allowing her to use her card for online shopping without a mobile phone, until they can offer an alternative authentication option that she has access to;
- Send Mrs R OTPs to her email address for her to use when she wants to set up a new payee (or amend an existing payee); and
- Pay Mrs R £350 for the distress and inconvenience caused to date by Santander's implementation of SCA which meant Mrs R was unable to do certain online banking and payment activities without a mobile phone.

If Mr and Mrs R accept this decision, my expectation is that Santander should pay Mrs R the £350 within 28 days of their acceptance.

With regard to the changes they've agreed to make so that Mrs R 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 Mrs R informed and to consider the impact of any further delay on her.

My final decision

My final decision is that I uphold Mr and Mrs R'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 R and Mrs R to accept or reject my decision before 18 April 2022.

Beth Wilcox
Ombudsman