DRN-2767134

The complaint

Mr S complains Santander UK Plc acted unfairly when it said he would need a mobile phone in order to continue using online banking.

What happened

Mr S has an account with Santander with a debit card. He's an elderly gentleman who's comfortable using online banking on his computer at home.

Santander emailed Mr S in July 2019 to say that it would be making changes to how its customers logged into online banking and authorised certain payments. Santander said that the changes meant its customers might have to confirm their identity through its mobile app or a one-time passcode ("OTP") sent to their mobile in certain circumstances. Santander said that it was making these changes as a result of new regulations that were coming into effect in September 2019 affecting the whole banking sector. Santander said that these measures were designed to help prevent fraud and increase the security of online payments.

Mr S complained to Santander about the changes it planned to make. He said that he didn't own a mobile phone – and didn't need one – and couldn't go into branch to carry out all the transactions he wanted to. He said he didn't see why Santander couldn't send an OTP to his landline. He said he couldn't see how that would put him at risk of fraud as he'd be logging onto his computer when the OTP arrived, and the OTP could only be used for limited purposes. He said he'd heard of other banks sending OTPs to landlines, and to email too.

Santander investigated Mr S's complaint and said that there were alternative ways he could access his account and make payments. Santander said, for example, that Mr S could use its telephone banking services and could go into branch. Santander said that it was aware other banks offered different options, but it required its customers to confirm their identity either through its mobile banking app or by providing an OTP sent to their mobile phone. In the meantime, Santander said that it was exploring options for customers who didn't have access to a mobile phone and would say more once it had made a decision about that. Mr S was unhappy with Santander's response so complained to us.

One of our investigators looked into Mr S's complaint and agreed that Santander hadn't acted fairly. Our investigator said that Santander should have offered Mr S alternative ways of authenticating himself that didn't rely on a mobile phone. So they recommended that Santander pay Mr S £250 in compensation and offer him alternative ways of authenticating himself.

Santander agreed to our investigator's recommendation of compensation and offered to send OTPs to Mr S's email address so that he could log onto online banking. In addition, Santander agreed to make an exception for Mr S so that he wouldn't be asked to authenticate himself if he used his card for online shopping whilst it came up with non-mobile options. However, Santander said that sometimes Mr S's transactions might be flagged for security. Santander wasn't willing to send OTPs to Mr S's landline or email address so that he could make payments to new payees using his online banking. Santander said that this wasn't a service it had offered before the changes. As Santander didn't agree to our

investigator's recommendations, I was asked to consider this complaint. Mr S was happy with what our investigator had said and sent us additional information explaining why he didn't have a mobile.

Having looked into Mr S's complaint, and to make sure both parties understood in detail my reasoning, I issued a Provisional Decision setting out my thoughts on this complaint in considerable detail. I agreed with the recommendation our investigator had made, namely that Santander should pay Mr S £250 in compensation and offer him an alternative way of authenticating himself.

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.

Santander told Mr S that it was making changes to the way its customers logged into online banking and authorised certain payments. Santander told Mr S 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.

Santander is right that new regulations came into effect in September 2019 – the Payment Services Regulations 2017 ("PSRs"). Santander 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 PSD2 – 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 Santander has gone about those checks – and the reliance it has placed on mobile phones to perform those checks – is at the heart of this complaint.

Santander's approach to implementing strong customer authentication - 2019

Santander told Mr S in July 2019 that it would be making changes to how he banked and shopped online as a result of new regulations. Santander told Mr S that:

- if he logged into his online banking, he'd be asked to provide his security number and user ID and then pass a second check. The nature of the second check would depend on whether he used Santander's mobile app or not. If he did, he'd be asked to use his fingerprint, face or security number. If he didn't, he'd be asked to use an OTP that would be sent to a device linked to him.

- he'd sometimes be asked to complete extra security if he was shopping online. The additional check would again depend on whether he used Santander's mobile app or not. If he did, he'd be asked to use his fingerprint, face or security number. If he didn't, he'd be asked to use an OTP that would be sent to a device linked to him.

In other words, Santander told Mr S that he'd soon have to pass either an "inherence" based check (his fingerprint or face), a "knowledge" based check (his security number) and / or a "possession" based check (providing the OTP) if he was logging into his online banking or shopping online. Santander told Mr S that if he needed an OTP it couldn't be sent to his landline or an email address – it would have to be sent to a mobile phone.

Why did Mr S complain?

Mr S has told us that he has a computer at home which he uses for his online banking – and that he finds online banking really useful. It allows him, for example, to download transaction details so he can answer questions about when he last paid someone or how often he's paid someone more easily. In addition, Mr S has told us that doesn't own a mobile phone and doesn't feel he needs one as he's never needed to make a call away from home. Finally, he's told us that he can't see how someone could use an OTP sent to his landline to perform fraud if he's sat at home using his computer when an OTP is sent to him. So, he's happy for Santander to send an OTP to his landline, or his email address.

Mr S has told us that his local branch is half a mile away and that he was having to go there to make payments to set up new payees and make payments to other payees because Santander won't send an OTP to his landline, or his email address. He's told us that this isn't always convenient, meaning he can't always do the transactions he wants to make. That's now changed – see below. But it meant that Mr S couldn't make payments to new payees using his online banking from home.

I accept that Mr S doesn't own or want a mobile phone – he has no need for one – and I've seen no evidence that he has another mobile device, such as a tablet. Nor would I expect him to do so given that he has no need for a mobile and is happy to use his computer at home in order to go online. So, I can understand why he complained about Santander's decision to send customers who don't use its mobile app OTPs to mobile phones only. He was worried it would mean he wouldn't be able to use online banking from home – putting him at a disadvantage.

It's important to note that Mr S isn't complaining about Santander'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. I don't think Mr S would have complained had Santander offered to send the OTP to his landline or email address so he could pass the extra checks Santander was introducing. In short, his only complaint is about Santander's decision to send the OTP he now needs to authenticate himself to mobile phones only.

*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".

Santander's approach to strong customer authentication – January 2022

Santander's approach to strong customer has, in its own words, "evolved" since 2019 when Mr S originally complained. By January 2022, for example, Santander had already agreed to send OTPs by email to consumers who want to log into their online banking and had already agreed to send OTPs by email to consumers who want to shop online. I've said what I think of Santander's "evolved" approach later on in this decision. But first it's right that I decide whether or not Santander's actions – when Mr S originally complained in 2019 – were fair and reasonable in all the circumstances.

Should Santander have done more for Mr S when he originally complained?

Mr S has told us that he doesn't own a mobile phone and doesn't feel he needs one. 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 Santander should have done more when Mr S 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 Santander to implement strong customer authentication – it's an important measure to help combat fraud. Nor do I think it was unfair or unreasonable of Santander to decide that it was going to use OTPs to help authenticate its customers. I do, however, think that it was unfair and unreasonable of Santander not to have offered Mr S alternative ways of authenticating when he complained. I'll explain why.

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. It follows that I don't think it was fair or reasonable that Santander didn't have an alternative way someone like Mr S could authenticate himself that didn't rely on a mobile phone when he complained. He should, in my opinion, have been able to log onto his online banking and make payments from his computer at home, rather than being forced to go to his local branch to do so – something I accept wasn't always convenient for Mr S.

Santander accepted that other firms were able to offer alternatives ways of authenticating – such as sending OTPs to a landline or by email – when Mr S complained, so I don't see why it couldn't have done so too. Santander, like the rest of the industry, had by then had several

years to prepare for strong customer authentication. Instead of coming up with alternative ways of authenticating – as many other businesses had by then – Santander suggested that Mr S use its telephone banking services or go into branch if he wanted to continue to access his account or make payments. I can see what Santander was trying to say here, but I think it's missed the point. The FCA has been clear that businesses should be offering customers alternative ways to authenticate themselves. What Santander was offering Mr S – when it suggested he could use its telephone banking services or go into branch instead – were alternatives to online banking rather than alternative ways to authenticate himself. For someone like Mr S, who wanted to be able to use online banking, wanted to be able to do so from his home and didn't always find it convenient to go into branch, I don't think that was fair and reasonable. I should add that suggesting to someone who wants to be able to use online banking from home, particularly someone who doesn't find it convenient going into branch, that they're able to continue banking by going into branch isn't particularly helpful. I should add also that Santander's insistence that Mr S use a mobile phone to authenticate himself feels like a failure to design a service in an inclusive way. He's an elderly gentleman, and like many elderly people doesn't own and doesn't want to own a mobile phone.

Has Santander done enough now that its approach has "evolved"?

Santander's approach to strong customer authentication has "evolved" several times since Mr S originally complained in November 2019 and having given a deadline to make any final comments on my Provisional Decision its approach has evolved again – more on this later. For example, Santander has for some time been willing to send OTPs to consumers by email if they're wanting to log onto their online banking or do online shopping.

Mr S has told us that he's not particularly interested in being able to do online shopping but being able to log onto his online banking from home is important to him. I'm satisfied that he's now able to log onto his online banking from home because Santander is now willing to send him an OTP by email which allows him to log on – it's an alternative that's viable for him. That's good to see. However, Santander took over eighteen months to come up with this alternative for Mr S – it started offering him this option in January 2021. That's disappointing given that many businesses were offering OTPs to email for logging on in 2019. That's also an option UK Finance recommended in the paper it published in October 2020. Santander chairs the steering group UK Finance set up to look into ways businesses could authenticate their customers, and in particular vulnerable customers. That makes Santander's failure to come up with alternatives sooner even more disappointing. Nevertheless, Santander now being willing to send OTPs by email for customers who want to log into their online banking solves one of the problems Mr S was having. But that's not the only problem he was having. He wanted to be able to make payments using his online banking from his computer at home. There the news wasn't until very recently so good.

Santander has told us more than once that it's not willing to send OTPs by email to customers who want to make a payment to a new payee using their online banking, or to a landline. I'll explain why, explain what it was offering and say whether I think what it was offering was fair and reasonable in all the circumstances.

Santander has used OTPs to authenticate its customers for years – it was one of the first banks to introduce them – it was using them as early as 2014. Santander has also included within its terms and conditions that its customers will need a mobile phone if they're going to make full use of online banking. I can understand why Santander introduced OTPs – authenticating customers using an OTP is an important tool in the fight against fraud. I can also understand why Santander would be particularly careful when it's deciding whether to accept an instruction to set up a new beneficiary or not as this is an area where fraudsters have been particularly active. But it doesn't follow, in my opinion, that Santander – even if it was "ahead of the game" in 2014 – didn't need to review its processes when it knew it would

have to implement strong customer authentication to check its approach was still up to date. The FCA's guidance has made it clear that businesses should offer customers alternative ways of authenticating whenever authentication is needed – as it is when a customer wants to make a payment from their online banking.

Santander told us than once that customers who don't have access to a mobile or its mobile banking app – for one reason or another – can still send payments to new payees using their online banking. In order to do so, customers have to call Santander's customer services department or a dedicated OTP helpline, and set up the new payee in question as a "trusted beneficiary". Once that's been done, payments to that beneficiary can be made without the need to authenticate, assuming the payments aren't, for example, flagged for security. Santander has said that calling its customer services department or its dedicated OTP helpline is an alternative way for its customers to authenticate. Santander has also said that it doesn't think asking customers like Mr S who don't have access to a mobile or its mobile banking app – for one reason or another – is unfair. I don't agree, and I'll explain why.

I accept that Mr S is able to call Santander's customer services department or its dedicated OTP helpline – he has a landline at home and is able to use it. He'd have to speak to an agent if he called either of these numbers as Santander doesn't offer an automated service. That means he'd have to wait for his call to be picked up, and he'd then have to go through telephone banking security, explain the reason for his call and then go through the process of setting up the new payee who he wanted to pay as a "trusted beneficiary". This would be the process for each new payee and it's a process that not only takes time, but a process that is far more likely to take longer than the time it would take if all he had to do was wait for an OTP to be sent to his landline or email address. In other words, it would be a more time-consuming process – and that's something I have to have regard to. Santander has told us that on average its customers need to set up a new beneficiary approximately eight times a year. I've seen nothing to suggest that Mr S sets up significantly more beneficiaries than that every year. So that's something I also have to have regard to. The process that I've just described – Mr S calling Santander's customer service department or its dedicated OTP helpline to set up a new payee is a process that appears to sit within telephone banking rather than online banking as far as I can see. In addition, the dedicated OTP helpline isn't available 24/7 – it's only available from 8am to 8pm Mondays to Fridays and from 8am to 6pm on Saturdays and Sundays. So, there will be occasions where Mr S cannot set up a new payee using the OTP helpline and would have to call Santander's customer services department instead which might be less optimal. Taking all of this into consideration, I have arrived at the conclusion that expecting someone like Mr S to call up and essentially go through a telephone banking process when they want the convenience of online banking is not fair or reasonable.

Santander's responses to me

Santander told me more than once that it was not willing or able to send an OTP to a landline or an email address so that one of its customers can authenticate when making a payment through their online banking to a new beneficiary. Santander also told me more than once that sending an OTP to a landline or an email address in such circumstances wasn't within its risk appetite. That's despite UK Finance recommending sending OTPs to a landline or an email address as viable options – work Santander must have been heavily involved in given that it chairs the steering committee overseeing this work. I didn't think that's good enough. I told both Santander and Mr S that I didn't think this is fair and reasonable in the exchanges I've had with them following my Provisional Decision. And I also asked them for comments on this. I've taken the comments I've received, which included a significant update from Santander – see below, along with all the other available evidence and arguments, into account when deciding what's fair and reasonable in all the circumstances.

I told both parties when I asked them for their final comments on my Provisional Decision that in this particular case I accepted that I couldn't require Santander to offer Mr S an option that it says it cannot offer and I don't have evidence to support it'd be practical or possible for it to do so; therefore, the only remedy I believed would adequately address this issue would be compensation. In its final comments on my Provisional Decision Santander has told me that it is now in the process of developing an OTP by email for customers who want to set up new payees, and that it will deploy this only as an exception for customers who cannot use a mobile phone. Santander has also told me that this is an option it's willing to offer Mr S. In short, it's now willing to offer Mr S what he asked for when he originally complained. That's good news and a significant development, although it's disappointing that it's taken Santander over two and a half years to get to this point.

Putting things right

I told both parties when I asked them for their final comments on my Provisional Decision that I thought an award of £350 in compensation would be appropriate in this case to reflect the inconvenience and frustration caused to Mr S. Santander agreed to that amount in its response to me in which it also let me know its approach has "evolved" again. I consider £350 to be fair compensation. So, I'm going to require Santander to pay Mr S £350 in compensation and to offer Mr S the OTP via email option it's developing once that becomes available in full and final settlement of this complaint.

My final decision

My final decision is that I require Santander UK Plc to pay Mr S £350 in compensation and to offer Mr S the OTP via email option solution it is developing once that becomes available in full and final settlement of this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 25 March 2022.

Nicolas Atkinson
Ombudsman