complaint

Mr and Mrs S are unhappy that Santander UK Plc debited their bank account for transactions they didn't make. Mrs S says she was tricked by fraudsters into handing over information which they then used to transfer funds out of their joint account.

background

Mrs S fell victim to a social engineering scam which involved "vishing". This is where a fraudster calls a consumer and uses a range of persuasive techniques to manipulate them into sharing personal information. Here the fraudster pretended to be from Mrs S's telecoms provider and convinced her to take certain steps and share information in order to gain access to her bank account and steal money from her and Mr S.

what happened?

Mrs S says she was at home unwell; she had been signed off from work and was feeling emotionally vulnerable. Mrs S was called by a fraudster pretending to be from her telecoms provider, saying there was a problem with her router. She says they'd had problems with their router in the previous weeks, so the call wasn't surprising.

Mrs S says she was told someone from California was hacking in to her router, and she needed to turn it off and back on again. Mrs S says she was directed to "run a scan" on her computer. She said the caller sounded like he was in a telecoms centre because of the noise in the background. She said all this convinced her she was talking to her genuine telecoms provider. It appears that during the call Mrs S was persuaded to download software on to her computer which gave the fraudster remote access. She's since said she didn't realise that's what she was doing at the time because she was just asked to type some letters into the computer. Mrs S says she was shown errors which linked to several of her online accounts, including shopping accounts and email accounts she and her husband genuinely used.

She said the caller knew she banked with Santander which is one of the things that led her to believe the caller was genuine. She says her direct debit for the telecoms service comes from the Santander account, so it strengthened her conviction that the caller was genuine and must have had access to her telecoms account.

Mrs S was persuaded to log in to her online banking. Mrs S has said she can't remember anything changing on the screen. She says she was told she would receive One Time Passcodes (OTPs) from Santander and these were "*to show Santander were authorising what was going on".* When these came through to her mobile phone, Mrs S relayed them to the caller. She received three codes. The text messages she received read:

'*This OTP is to AMEND A PAYEE on a payment. Don't share this code with anyone. Call us immediately if you didn't request this [OTP CODE].'*
Shortly after sharing these codes, Mrs S's conversation with the caller ended.

The fraudster used these codes to change the details of three existing payees (name, account number and sort code) on Mr and Mrs S's joint account, and attempted transfers totalling £18,338. The fraudster also transferred money between Mrs S's other linked accounts, her savings and sole current account, totalling £800.

Nearly an hour after Mrs S first logged into her online banking, she received an "Adeptra call" (an additional security call) from Santander. This call was prompted by Santander's fraud systems which flagged three of the transactions as suspicious. The call was to verify with Mrs S that she had authorised these payments from her account. She responded to the automated call saying she hadn't authorised any payments from her account. Because of her response to the automated call she was transferred to Santander's fraud department, and she explained what had happened earlier. The following are relevant extracts from the call between Mrs S and Santander:

"… they made me go through stuff on my computer. Is my computer not safe now either? [call handler advises Mrs S to turn off computer while he tries to stop pending payments] … "I went through a [telecoms provider] website … I just don't understand … I even phoned [telecoms provider] from my mobile while this was going on and he said 'I know that you've just phoned [telecoms provider]' … 'cos I suspected it might have been a scam and this is what I just don't understand … They just said to me someone in California is hacking on to your router, can I unplug my router and turn it back on again. And then they asked me to go on to a [telecom provider's website] and do a scan, and it just looked like it was a Microsoft scan. And I've just been completely had. And so I phoned [telecoms provider] on my other phone because I didn't trust it, and he said to me I know you've just tried to ring [telecoms provider]. So I'm like, did they hack my phone as well. I just don't understand … "He sounded like he was in a massive [telecoms provider] call centre; there were so many people in the background …"

"I don't know what I downloaded … Is it still safe to log on? … I kept questioning him because I just didn't trust it but he had all the answers … We've had trouble with the [telecoms provider] … And I've had a couple of these OTPs 'cos he said he was trying to clear stuff on the system but obviously that was how he got into my bank account … [pause] quite clearly your message says don't share with anybody … [call handler advises restrictions have been placed on account, advises Mrs S to get laptop professionally cleaned, and explains process - call ends]."

Santander was able to stop some of the payments at this time but Mr and Mrs S suffered losses of £9,760 from their joint account.

Below are the timings of the online banking activities during the scam, according to Santander's online banking records:

Date	Time	Online activity	Amount	Recovered?
13/12/16	*11.52*	*Mrs S logged into online banking*		
13/12/16	*12.09*	*First OTP sent to Mrs S and was used to amend a payee at 12.10*		
13/12/16	*12.12*	*First payment transferred out of the account (to payee 1)*	*£4,880.00*	*no*
13/12/16	*12.18*	*Second payment transferred out of account (to payee 1)*	*£4,788.00*	*yes*
13/12/16	*12.29*	*Second OTP sent to Mrs S and was used to amend a payee at the same time*		
13/12/16	*12.31*	*Third payment transferred out of the account (to payee 2)*	*£4,880.00*	*no*
13/12/16	*12.38*	*Third OTP sent to Mrs S and was used to*		

		amend a payee at 12.39		
13/12/16	*12.40*	*Fourth payment transferred out of the account (to payee 3)*	*£2,900.00*	*yes*
13/12/16	*12.24*	*Transfer of money from Mrs S's savings account into the joint account*	*£400*	
13/12/16	*12.43*	*Transfers of money from Mrs S's sole current account into the joint account*	*£400*	
13/12/16	*12.45*	*Fifth payment transferred out of the account (to payee 2)*	*£890.00*	*yes*
				£9760.00

Mr and Mrs S do not dispute that Mrs S gave over one time passcodes (OTPs) to the fraudster. But they think the system in place at the time for amending existing payees was inadequate, and say this is demonstrated by others falling for the same scam. Mr and Mrs S want to know how the fraudster was able to change the name and account details of three existing payees and make large transfers to them without detection or suspicion by Santander.

Santander didn't refund Mr and Mrs S. It said the transactions occurred after Mrs S allowed a third party to remotely access her computer and online banking. This gave the third party full access to Mr and Mrs S's bank accounts. It also said the transactions were authorised using OTPs contained within text messages which were sent to Mrs S's registered mobile number, and which were then entered into online banking by the fraudster.

Santander offered Mr and Mrs S £100 compensation for poor complaint handling as it didn't respond to the complaint when it was first raised in January 2017.

As Mr and Mrs S weren't happy with Santander's final response so they referred their complaint here. One of our investigators looked into things. He concluded that because Mrs S had allowed the fraudsters access to her online banking (albeit unwittingly) and given away the OTPs, which allowed the fraudster to carry out the transactions, Santander didn't need to refund the transactions.

Mr and Mrs S did not agree with the investigator's findings and asked for an ombudsman to review their complaint, so it has been passed to me.

response to my provisional findings

on 23 November 2018 I issued a provisional decision on Mr and Mrs S's complaint. After considering all the evidence and arguments presented by both sides, I was minded to conclude that:

- Mrs S did not authorise the transactions in question;
- Mrs S had not acted with gross negligence;
- Santander should fairly and reasonably refund the money obtained from Mrs S by the fraudster, plus interest at the rate he would have received had the money remained in Mr and Mrs S's joint account; and

- Santander should pay Mr and Mrs S £300 for the trouble and upset they experienced.

Mr and Mrs S's representative responded and in summary said:

- Santander should bear a substantial responsibility for this fraud because they had failed to identify the security flaw in their authorisation procedure – its OTP system was flawed and created a loophole for fraudsters to exploit.

- In light of this clear failing on Santander's part I believe that Mr and Mrs S should be awarded a significantly higher rate of interest than they would have received had the money not been moved from the account. Whilst they had no stated plans for these funds, they lost the opportunity of investing them and have had to live for nearly two years not knowing if they would ever recover their money.

Santander also responded to say it had nothing further to add and accepted the findings reached in my provisional decision.

my findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint. As both parties accept on the whole accept my provisional findings I see no reason to depart from these so I'll set those out again here and I'll address the additional points raised by Mr and Mrs S's representative.

my provisional findings

The rules of our service mean that I have 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's 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.

I've summarised below what I consider to be the relevant regulations and account terms, and I've taken them into account when deciding this complaint.

relevant considerations

Santander as an FCA regulated firm provided a current 'deposit' account. As such the FCA's overarching Principles for Businesses apply including the requirement to pay due regard to a customer's interests and treat them fairly (Principle 6).

The transfers from Mr and Mrs S's account were made in December 2016. So of particular relevance to my decision about what is fair and reasonable in the circumstances of this complaint are the Payment Services Regulations 2009 (PSR 2009). I think these sections of PSR 2009 are of particular relevance here:

Consent and withdrawal of consent

55.—(1) A payment transaction is to be regarded as having been authorised by the payer for the purposes of this Part only if the payer has given its consent to—

(a) the execution of the payment transaction; …

Obligations of the payment service user in relation to payment instruments

57.—(1) A payment service user to whom a payment instrument has been issued must—

(a) use the payment instrument in accordance with the Terms and Conditions governing its issue and use; and
(b) notify the payment service provider in the agreed manner and without undue delay on becoming aware of the loss, theft, misappropriation or unauthorised use of the payment instrument.

(2) The payment service user must on receiving a payment instrument take all reasonable steps to keep its personalised security features safe.

Evidence on authentication and execution of payment transactions

60.—(1) Where a payment service user—

(a) denies having authorised an executed payment transaction; or
(b) claims that a payment transaction has not been correctly executed,

it is for the payment service provider to prove that the payment transaction was authenticated, accurately recorded, entered in the payment service provider's accounts and not affected by a technical breakdown or some other deficiency.

(2) In paragraph (1) "authenticated" means the use of any procedure by which a payment service provider is able to verify the use of a specific payment instrument, including its personalised security features.

(3) Where a payment service user denies having authorised an executed payment transaction, the use of a payment instrument recorded by the payment service provider is not in itself necessarily sufficient to prove either that—

(a) the payment transaction was authorised by the payer; or
(b) the payer acted fraudulently or failed with intent or gross negligence to comply with regulation 57.

Payment service provider's liability for unauthorised payment transactions

61. Subject to regulations 59 [Notification of unauthorised or incorrectly executed payment transactions] *and 60, where an executed payment transaction was not authorised in accordance with regulation 55, the payment service provider must immediately—*

(a) refund the amount of the unauthorised payment transaction to the payer; and
(b) where applicable, restore the debited payment account to the state it would have been in had the unauthorised payment transaction not taken place.

Payer's liability for unauthorised payment transactions

62.—(1) Subject to paragraphs (2) …, the payer is liable up to a maximum of £50 for any losses incurred in respect of unauthorised payment transactions arising—

(a) from the use of a lost or stolen payment instrument; or
(b) where the payer has failed to keep the personalised security features of the payment instrument safe, from the misappropriation of the payment instrument.

(2) The payer is liable for all losses incurred in respect of an unauthorised payment transaction where the payer—
(a) has acted fraudulently; or
(b) has with intent or gross negligence failed to comply with regulation 57.

consent

Regulation 55 says that the payer must give consent, and it "*must be given in the form, and in accordance with the procedure, agreed between the payer and its payment service provider*". The payment services directive itself (which PSR 2009 implements) says "*In the absence of such consent, a payment transaction shall be considered to be unauthorised*." But neither PSR 2009 nor the FCA's 2013 guidance on PSR 2009 provide a definition of "consent".

I therefore think it is fair, when considering whether consent was given, to apply the common definition of consent, which is to give permission for something to happen.

gross negligence

Whether a customer has acted with "gross negligence" is something that can only be assessed on a case by case basis taking into account all the circumstances. The term is not defined in PSR 2009 nor in the first Payment Services Directive. However, recital 72 of the second Payment Services Directive provides as follows:

"In order to assess possible negligence or gross negligence on the part of the payment service user, account should be taken of all of the circumstances. The evidence and degree of alleged negligence should generally be evaluated according to national law. However, while the concept of negligence implies a breach of a duty of care, gross negligence should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness; for example, keeping the credentials used to authorise a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties…"

Reflecting this, the FCA, in its document setting out its role under the Payment Services Regulations 2017, says:

"*… we interpret "gross negligence" to be a higher standard than the standard of negligence under common law. The customer needs to have shown a very significant degree of carelessness.*"

Although neither of these is directly relevant to this complaint, they are of value as a relevant consideration in the absence of contemporaneous interpretative guidance, and because they inform the meaning of a concept that has been in place for some time (in the Banking Code).

When considering gross negligence in a commercial contract context, Mance J in Red Sea Tankers Ltd v Papachristidis (The "Ardent") [1997] 2 Lloyd's Rep 547, 586 said:

"If the matter is viewed according to purely English principles of construction, … "Gross" negligence is clearly intended to represent something more fundamental than failure to exercise proper skill and/or care constituting negligence… as a matter of ordinary language and general impression, the concept of gross negligence seems to me capable of embracing not only conduct undertaken with actual appreciation of the risks involved, but also serious disregard of or indifference to an obvious risk."

Negligence is often referred to as a failure to exercise reasonable care. But as I have described above, gross negligence suggests a lack of care that goes significantly beyond ordinary negligence. So I have to consider whether what Mrs S did fell so far below the standard expected of a reasonable person that it would be fair to say she failed with gross negligence to keep her personalised security details safe or to comply with the Terms and Conditions of her account.

the Terms & Conditions of Mr and Mrs S's account

Santander has referred to its Terms and Conditions when considering Mrs S's actions.

The following are extracts from the general Terms and Conditions applicable to Mr and Mrs S's joint account at the time. These Terms and Conditions broadly reflect the provisions contained in the PSRs 2009.

7. "*your remedies for unauthorised payments a) if you notify us that a payment was not authorised by you, we will immediately refund your account with the amount of the unauthorised payment taken….. b) before we refund your account, we are entitled to carry out an investigation if there are reasonable grounds for us to suspect that you have acted fraudulently, deliberately or have been grossly negligent. We will conduct our investigation as quickly as possible and may ask you to reasonably assist in that investigation."*

9. "*you must keep your Personal Security Details secure and follow the safeguards in this document and on santander.co.uk to keep your Personal Security Details, PIN, card and chequebook secure… The care of your chequebooks, cards, PINs, Personal Security Details and selected personal information is essential to help prevent fraud and protect your account. To ensure this you must: … not disclose your PIN or Personal Security Details to anyone else, not even a member of Santander staff; and… only enter your Personal Security Details where you are requested to do so by an online banking screen. c) we may debit your account with any amount refunded under Condition 7.2 a) in Section 2A where we subsequently become aware that the payment authorised by you or that any of the circumstances "*

9.7 "the care of your chequebooks, cards, PINs, Personal Security Details and selected personal information is essential to help prevent fraud and protect your account. the ensure this you must:…c) always take reasonable steps to keep your cards safe and your PIN, Personal Security Details and selected personal information secret and dispose of them safely. f) not disclose your PIN and Personal Security Details to anyone else, not even a

member of staff. h) only enter your Personal Security Details where you are requested to do so by an online banking screen; i) act on any further instructions we give you to ensure that your online banking is secure. Any instructions will reflect good security practice, taking account of developments in e-commerce."

13. "*in each case we have to show that you acted fraudulently, deliberately or with gross negligence or that you failed to notify us as required*."

13.3 "*we have to prove: any allegation of fraud; or that you were grossly negligent in failing to follow any of the safeguards listed in 9.7…"*

Santander also referred us to its online banking terms when considering Mrs S's actions in giving over OTPs to the fraudster:

"To access the online service, customers need to accept the Conditions of use. They state at 11.1.6 – 'Whenever you use the One Time Passcode functions you must take all reasonable precautions to prevent anyone else from accessing your confidential information including the One Time Passcode(s) that will be sent to you. You must never disclose your One Time Passcode verbally to any individual even if they claim to be our employees or agents or the Police."

key questions

In my view the above relevant considerations mean that, if the transactions were unauthorised, it would be fair and reasonable for Santander to refund the amount stolen from Mr and Mrs S, unless Mrs S, with intent or gross negligence, failed to comply with the Terms and Conditions of the account and the obligations set out in Regulation 57.

The reasons given by Santander for deciding to not refund the amount stolen from Mr and Mrs S are not clear. Santander in its final response to their complaint simply said it was because "*you allowed a third party to remotely access your computer and online banking. This has given the third party full access to your bank accounts. The transaction has also been authorised using our One Time Passcode service. Text messages were sent to your registered mobile phone number and entered into online banking.*"

Santander hasn't made it clear on what basis it is holding Mr and Mrs S liable for the disputed transactions. In these circumstances I think there are two key questions relevant to my consideration about what is fair and reasonable in the circumstances:

1. Were the disputed transactions authorised by Mrs S? and;

2. If they weren't, can Santander demonstrate that Mrs S failed with intent or gross negligence either to comply with the Terms and Conditions of her account or to keep her personalised security details safe?

Though there is naturally some overlap of events when answering these two questions, I will approach them in this order. But before I do so I'm going comment on Santander's investigation in the initial hours and weeks after the scam.

Santander's investigation

I've listened to the calls between Mrs S and Santander, in particular the first call that Mrs S makes where she responded to the Adeptra call. This is where Mrs S realises she's just been the victim of a scam. This is the most reliable recollection of events by Mrs S; it's just happened in the moments before. So I think it's reasonable to rely on what she said during that call about how the scam unfolded.

Mrs S gives information piecemeal as the call handler quickly tries to stop the payments. In that first call, however, the call handler in Santander's fraud department doesn't give Mrs S the opportunity to fully recount what has just happened, which I appreciate is a competing priority with trying to act quickly to stop and recover the payments.

Santander called Mrs S back over two weeks later and asked some questions about what happened during the scam. But again she isn't asked to recount all the steps that the fraudster asked her to go through, and what information she gave over and why. I think Santander should've asked Mrs S more questions at the time, to piece together what exactly happened. Because it didn't do this, information is missing and the recollections from Mrs S aren't as full as I'd like. It's now not possible to know exactly what happened during the scam.

As I've said, I've listened to the calls to piece together what I think most likely happened at the time. And I'm satisfied that I have enough information to reach a fair and reasonable conclusion on this complaint. I've had to re-create what I think most likely happened based on these calls, and Mrs S's later recollection of events and the technical information provided from Santander to show the online banking activity.

were the disputed transactions authorised by Mrs S?

On the balance of evidence I'm not persuaded that Mrs S authorised these transactions from her joint account with Mr S. I'll explain why.

As I've said I don't know exactly what steps were taken by Mrs S, but it appears as though she gave the fraudster remote access to her computer. During the first call with Santander she said, *"… they made me go through stuff on my computer. Is my computer not safe now either?*" The Santander call handler asked if the fraudster had remote access to her computer, and Mrs S says she went through what looked like the genuine telecoms provider's website.

A representative for Mrs S wrote to us in July 2017 and detailed Mrs S's recollections of events. The representative said the fraudster instructed Mrs S to type a number of things into her computer – I think this is when Mrs S believed she was running a scan on her computer – but this is when I think the fraudster actually gained remote access to her computer. Based on what I've heard during her calls with Santander I'm persuaded that, at the time, she didn't know that taking the steps she did, to run the scan, actually gave the fraudster remote access to her computer.

Mrs S accepts she gave over the OTPs to the fraudster. She says she thought he needed these to clear a virus from her online banking. Given what happened next, it's clear the fraudster used these codes to amend existing payees on the account. The fraudster then transferred money out of Mr and Mrs S's bank account to payees unknown to them.

However, there is no evidence to show that, at any point during the call with the fraudster, Mrs S knew that any payments were going to be made from the joint account. Mrs S says she was told the OTPs were "*to show Santander was authorising what was happening"* and "*to clear stuff off the system*" and at the time she thought she was talking to someone from her telecoms provider. I don't think she had any reason to believe the process she thought was underway (running a scan and clearing her computer), involving her telecoms provider, would involve any money being taken from her account. I also note that when she received the Adeptra call she responded "no" when asked if she'd authorised payments to leave her account. I think it unlikely that would have been the case if Mrs S had given her permission (i.e. consented) for payments to be made from her joint account.

Mrs S recalls that she didn't enter the OTPs into her online banking, she gave these to the fraudster - and I think that's likely given her recollections, and the fact that a fraudster with remote access to her online banking would have been able to enter the OTPs themselves. I don't think she was aware that any payments were being made from her account. On balance I'm persuaded Mrs S didn't consent to or authorise these transactions to be made from her joint account.

So, my starting point here is that it wouldn't be fair and reasonable for Mrs S to be held liable for these transactions – which I think are more likely than not to have been unauthorised - unless she has failed with intent or gross negligence to comply with the terms and conditions of her relationship with Santander and the obligations set out in the PSR 2009.

did Mrs S fail with gross negligence either to comply with the Terms and Conditions of her account, or to keep her personalised security details safe?

Mrs S was tricked by a fraudster into allowing remote access to her computer, and then persuaded to log in to her online banking. Mrs S was also then tricked into handing over three OTPs which allowed three existing payees to be amended, effectively making them into entirely new payees. However, on the balance of evidence, I don't think it would be fair and reasonable to say that, in falling for these tricks and failing to keep her security details safe, Mrs S was grossly negligent. I'll explain why.

As I set out earlier, negligence is often referred to as a failure to exercise reasonable care. I think it is fair to say that gross negligence involves a degree of negligence that is higher than ordinary negligence. That is consistent with what has been held by the courts in a commercial contract context (as mentioned, Mance J held that ""*Gross" negligence is clearly intended to represent something more fundamental than failure to exercise proper skill and/or care constituting negligence"),* and the FCA's guidance, which says that gross negligence is a *"higher standard than the standard of negligence under common law".*

I've thought carefully about the actions Mrs S took in the circumstances here, and whether what she did, fell so far below the standard of a reasonable person that it would be fair to say she failed with gross negligence to keep her personalised security details safe or to comply with the Terms and Conditions of the account.

Gross negligence isn't an abstract concept. It's important to take into account all the circumstances when considering whether an individual's actions amount to gross negligence. The scam here involved "*social engineering*", where the fraudsters use a range of sophisticated techniques to trick, deceive and manipulate their victims into giving out confidential information. Here Mrs S was made to believe she was talking to a genuine company she'd had previous dealings with and that she needed to act quickly to protect herself from an attack on her email and bank accounts. So I've thought about Mrs S's actions in that context, and considered each thing she did in turn:

- Mrs S had recently had problems with her telecoms provider and says she had spoken with the genuine telecoms provider, in the weeks before the fraudulent call. She says the fraudster knew information about her and it sounded like they were calling from a genuine call centre; and she says "*he had all the answers*". Although she had her doubts during the call, she was reassured when the caller appeared to know she was trying to call the telecoms provider from her mobile. So I can understand why all of this together caused Mrs S to think she was talking to her genuine telecoms provider. And I'm satisfied that in this instance Mrs S was entitled to think she was talking to her telecoms provider and didn't expect them to scam her. I think many reasonable consumers would have been similarly convinced in the circumstances.

- When she downloaded the remote access software Mrs S says that she thought she was running a scan on her computer, that she was directed to a website which she says displayed the telecoms provider's logo, and that it looked to be genuine. I have no reason to doubt her recollection about this. It wasn't until after the fraud had happened that she realised she had inadvertently given the fraudster remote access to her computer. Given that Mrs S thought she was following the instructions of her telecoms provider I don't think it was unreasonable for her to believe that she was only running a scan.

- Mrs S was told her email accounts had been affected and the fraudster then *"coaxed her to go into her online banking*". She did so quickly and she thought she was proactively protecting her online banking. I acknowledge that, when considering the situation with the benefit of hindsight, you might ask how Mrs S's telecoms provider would know her bank account was also under attack. But this in itself doesn't lead me conclude that Mrs S was *grossly* negligent in failing to comply with either the terms of the account, or her obligations under the PSRs to take all reasonable steps to keep her personalised security details safe. In the context that Mrs S thought she was speaking with someone with technical expertise, from a company she trusted, who had seemingly just shown her errors with her other online accounts, I can understand why she believed the fraudster, when he said it was necessary for her to log into her online banking. And I think a reasonable person would've acted in a similar way.

- The fraudsters told Mrs S to expect codes from her bank. She says they told her these were "*to show Santander were authorising what was going on*". So she says she wasn't alarmed when she received the text messages from Santander containing the OTPs, and she says she didn't question the wording of the text messages as they didn't say that money or any amount would be transferred from the account. I have thought about whether the wording of the messages should have alerted Mrs S to what was going on. After all, she thought the code was to "*clear stuff"* and not to "*amend a payee*". It could be said that Mrs S showed a lack of care by providing the fraudster with these codes. The messages did say, "*Don't share this code with anyone*". But it does not necessarily follow that Mrs S was *grossly* negligent.

- Listening to her conversation with Santander on the day of the fraud, I don't think she fully read the text messages until she was recalling what had happened. I think it's relevant that she said *"I had a couple of OTPs as he said he was trying to clear stuff off the system but obviously that was how he got into my bank account".* Of course, that's not how the fraudster got into her bank account; that was achieved by persuading Mrs S to log in herself. So I think it's clear from that call that Mrs S didn't understand how the fraudster had accessed her account.

- With the benefit of hindsight you might ask why Mrs S did not question the wording of the text and heed the warning not to share the code with anyone. However, I am mindful that by the time the messages came through, Mrs S firmly believed that she was talking to a representative of a trusted telecoms provider. The fraudster made it seem that they were in contact with Santander – had Santander's authority even – because they anticipated Mrs S being sent the text messages. She thought she was following instructions aimed at protecting her bank account. Mrs S says the fraudsters told her they needed the code as it was being used "*to clear stuff of the system".* In the environment the fraudster created I can understand why she simply followed the fraudster's instructions. She'd also been on the telephone to the fraudster for a significant length of time, was worried about the security of her online accounts, and felt pressure to act. In similar circumstances I think a reasonable person would've acted in the same way that Mrs S did here.

- Santander's Terms and Conditions at 13.3 make it clear that it bears the responsibility for proving that Mrs S failed with gross negligence to keep her personalised security details safe. Although it has shown that Mrs S logged into her online account whilst the fraudster had access to her computer, and that she gave three OTPs to the fraudster, they haven't persuaded me that her actions fell so far below what a reasonable person would do in the circumstances to amount to gross negligence.

I appreciate that the OTPs were a key security tool and Mrs S should not have revealed them to the fraudster. But the test for me to consider here is whether Mrs S was grossly negligent in failing to comply with the Terms and Conditions of her account, or to keep her personalised security details safe. In order to be grossly negligent Mrs S needs to have shown a very significant degree of carelessness. Here Mrs S was persuaded to divulge security features to a fraudster as part of sophisticated and successful scam.

For the reasons I've given I think a reasonable Santander customer may well have taken the same steps that Mrs S did in sharing the details the fraudster convinced her to share. This was not an obvious risk to a reasonable person in Mrs S's position because she had been socially engineered into thinking that what she was doing was preventing harm to her computer and online accounts. So I'm not currently minded to find Mrs S was *grossly* negligent in these circumstances.

additional points raised by Mr and Mrs S's representative

Mr and Mrs S's rep has said that because he believes Santander's OTP "amend payee" function is flawed it should "*bear a substantial responsibility for this fraud"*. And he's said that in light of this clear failing by Santander he believes Mr and Mrs S should be awarded a significantly higher rate of interest than they would have received had the money not been moved from the account. But it's for me to consider the individual complaint before me to determine what I think is fair and reasonable in the circumstances. Having done that I've found that Santander should return all the money lost through the scam to Mr and Mrs S, plus interest and a compensation payment. So I don't think I need to make any further award here for the reasons set out by Mr and Mrs S's rep.

As I've upheld the complaint I would usually look to put Mr and Mrs S back in the position they would've been in if things had happened as they should and to award fair compensation. And I can look to compensate Mr and Mrs S for being "deprived" of money – that is, not having the money available to use. I can also tell the business to pay interest on top of the money award for the period Mr and Mrs S were out of pocket.

Here I've awarded the rate of interest that was paid on the account. That's because Mr and Mrs S's money was in a higher paying interest rate account than other standard current accounts. Mr and Mrs S's representative has said they didn't have any specific plans for the money but lost out on the opportunity to invest. But Mr and Mrs S haven't said or provided me with anything to suggest they had any plans for this money or had to borrow money or had done so at a higher rate of interest to cover their losses here. I've also considered that the money had been in the account for some time prior to the fraud. Taking all of this into account I'm persuaded it's likely the money would've remained in that account if the fraud had not occurred so I'm satisfied the account interest rate is the right award here.

Mr and Mrs S rep also says they had to live for nearly two years not knowing if they would ever recover their money and I accept that would have caused them some upset. This is why I made a recommendation for compensation of £300, which I think is fair in the circumstances of the complaint.

putting things right

For the reasons given, I do not think it was fair and reasonable for Santander not to refund the amount stolen from Mr and Mrs S's joint account.

I now direct Santander to:

- refund Mr and Mrs S's joint account with £9,760; and

- pay interest on that amount at the respective account interest rates, from the date of the withdrawals to the date of settlement. If Santander deducts tax from the interest

element of this award, it should provide Mr and Mrs S with the appropriate tax deduction certificate.

- This has been a very worrying time for Mr and Mrs S. Mrs S was the direct victim of the scam and was clearly distressed on the two occasions Santander called her to discuss the events with her. Having considered the matter as a whole and the impact Mr S and in particular Mrs S have described, I think it would be fair for Santander to pay Mr and Mrs S a further £300 compensation for the trouble and upset they experienced.

Under PSR 2009, and the Terms and Conditions of the account which reflect that legislation, Santander is entitled to hold Mr and Mrs S responsible for the first £50 of their loss. If it intends to do this, it can take this amount from the £9,760 before adding the interest element.

my final decision

As set out above I uphold Mr and Mrs S's complaint against Santander UK Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr and Mrs S to accept or reject my decision before 26 April 2019.

Sophia Smith
ombudsman