Some aspects of this decision have been redacted for security purposes.

complaint

Mr B complains that Santander UK Plc won't refund £12,310 of payments from his account that he says he didn't authorise.

background

Mr B held a 1-2-3 current account with Santander. In March 2017 he was the victim of a scam known as "*smishing*" (this is where a fraudster sends an SMS text message to a customer and it appears to come from their bank). It is not in dispute that what happened to Mr B was an act of fraud, so I have used the term '*fraudster*' throughout to refer to the third party involved.

Mr B says that, on 2 March 2017, he received a text message which appeared to come from Santander. The message looked like it had been sent from the same phone number that he'd previously received messages from Santander on. The message came up on his phone as being from 'Santander' and joined the Santander 'message thread' – alongside the messages he had genuinely received from the bank. He therefore assumed that the message had in fact been sent by Santander. The message read:

"*Santander has noticed your debit card was recently used on 02-03-2017 15:59:03 at APPLE ONLINE STORE for 1,976.00 GBP. If not you please urgently call fraud prevention on XXXXXXXXXX or Intl XXXXXXXXXX. Do not reply by SMS*".

Mr B had recently signed up for 'Apple Pay' (a system allowing a consumer to use their phone, rather than their physical debit or credit card, to make purchases). He thought the message might be connected to that. As he didn't recognise this transaction, he called the "*fraud prevention*" number given and was asked a series of questions.

Mr B can't recall exactly what questions he was asked, or what answers he gave to those questions. Mr B's recollection of this interaction is that they *"went through the normal security etc. and worked through the issue of the Apple payment".* It seems that whilst talking to Mr B, the fraudster accessed Mr B's online banking facility and through that his account.

Whilst in Mr B's online account, the fraudster changed the account details for one of Mr B's existing payees. The fraudster changed the details to such an extent that it altered the account number and sort code of an existing bill payment.

Mr B, who says he was still on the telephone to the fraudster at this point, then received a One Time Passcode (OTP) message to his phone from Santander. Mr B says the fraudster pre-empted the receipt of this message by telling him he would receive the code shortly, via text message. Mr B says that the fraudster told him that he would need to *"know the OTP"* in order to clarify it was Mr B on the phone and that he was *"not being hacked".* And that in doing this, it would stop the Apple payment. Mr B recalls that *"as soon as he said this the text came through".*

The OTP message arrived in the same thread as the original message from the fraudster and the genuine text messages that Mr B had previously received from Santander. In view of this, Mr B said it *"rose no alarm bells"* for him.

The message 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 XXXXXXXX*".

Mr B gave the code to the fraudster and, shortly afterwards, £12,300, along with a second payment of £10.00, was transferred out of his account to the newly 'amended' payee.

Mr B was still on the telephone to the fraudster when Santander sent him an automated fraud prevention voicemail (known as [redacted] call) asking him to call them back. Mr B says that the fraudster, once again, pre-empted this by telling him that he was going to send the voicemail to him. Mr B's recollection of this is *"as soon as he finished saying the words my phone buzzed".*

The voicemail contained the following:

[redacted]

Mr B says that the fraudster asked him to listen to the voicemail and to give him the *"information"* contained within it. He said that he did as instructed because the fraudster told him the information was necessary to stop the suspicious payment. Mr B added that *"because of the nature of the text message and official voicemail, I had no reason to think otherwise".*

The following afternoon, on 3 March 2017, a member of staff from Santander's fraud and security team called Mr B to ask him whether he had made the transactions for £12,310. They left him a voicemail asking him to call back. When he did so and confirmed that he hadn't authorised the transactions, a fraud investigation began.

Santander was only able to recover £35 from the recipient bank - it says the money was moved very quickly and used to buy foreign currency. It refused to reimburse Mr B the rest as it was satisfied that he'd authorised the disputed payment by using the OTP. It also explained that Mr B had responded to the [redacted] call, on 2 March 2017, confirming via its automated system that he recognised the transactions.

Santander has provided the following transcript of what happened when the [redacted] call was responded to:

[redacted]

[redacted]

Mr B has no recollection of responding to a voicemail from Santander until 3 March 2017. This is when he called Santander back, in response to the message left by a member of staff (not an automated message), and spoke with someone in the fraud and security team.

Specifically, Mr B does not remember replying to an automated voicemail on 2 March 2017 – other than to provide the fraudster with the *"information"* contained within it as instructed. Mr B has been clear that he does not remember responding to any automated questions about the transactions using his phone key pad. On this, he has said *"I do not remember that call at all".*

For clarity, this appears to be the approximate timeline of what happened on 2 March 2017:

16:07	Mr B received a text message which looked like it had come from Santander
16:11	The fraudster logged on to Mr B's online banking
16:17	Mr B received an OTP by text message

16:19	Payment made to amended payee for £12,300
16:20	[redacted] call attempted, voicemail left for Mr B, followed shortly by unsuccessful inbound [redacted] call
16:40	Payment made to amended payee for £10.00, followed shortly by unsuccessful inbound [redacted] call
16:46	Someone responded to the [redacted] voicemail confirming transactions as genuine
16:48	The fraudster logged off from Mr B's online banking

In its final response to Mr B's complaint, Santander said that it makes significant efforts to educate customers about potential scams. And that its message to customers is that they should never disclose their security details. Santander also said it had sent two emails to Mr B, informing him about the threat of "*smishing*" scams in November 2016 and January 2017, but that he had not read them.

In respect of the [redacted] calls, Santander said the following to Mr B:

"At 16:20, our Automated Fraud Monitoring System attempted to contact you to validate this payment as genuine, however they were unable to get through on your registered mobile. At 16:40, the fraudster made a further payment for £10.00 to the same destination account. At 16:40, we tried to make further contact with you to authorise the payment, but the line was disconnected.

These contacts were made after your registered number satisfied our internal SIM swap checks. At 16:46 we then received confirmation via our Automated Fraud Monitoring System that the Bill Payment was genuine. However, had the OTP not been provided, the transactions would not have debited."

my provisional decision

On 25 May 2018 I issued a provisional decision on Mr B's complaint. After considering all the evidence and arguments presented by both sides, I was minded to conclude that:

- Mr B did not authorise the transactions in question
- Mr B had not acted with gross negligence
- Santander should fairly and reasonably refund the money obtained from Mr B by the fraudster (where it had not done so already), plus interest at the rate he would have received had the money remained in his 1-2-3 account.

I attach a copy of my provisional decision to this final decision, which forms part of this final decision, and details in full how and why I reached those conclusions.

Santander's response to my provisional decision

Though Mr B accepted my provisional decision, Santander did not. It took this position for a number of reasons.

- It agreed that the payments would be unauthorised if Mr B was not the person who made the [redacted] call. However, it felt that, if it was Mr B who made the call, then, given its view that the wording in the [redacted] message is *"clear and expressly refers to a payment and its amount",* the payment would have been authorised. Essentially, Santander believes it would have been entitled to reject this complaint if Mr B made the [redacted] call.

  In light of this, Santander expressed its disappointment that Mr B has not been *"pressed harder to obtain evidence in the form of itemised phone records".* In Santander's view, the investigation and analysis regarding whether the transaction was authorised accordingly remained *"incomplete".*

- Santander felt it was unclear, from my provisional decision, if the objective test for whether Mr B was *"negligent to a degree which fell well short of the standard of care to be expected of a reasonable person, placed in the same circumstances"* had been applied.

- After reviewing the sequence of events that led to Mr B being tricked by the fraudster, Santander considered most customers' suspicions would have been aroused. On this, it made the following observations:

  "First, the initial text message to the customer indicated that a payment to the Apple store had already been made. The customer was however led to believe by the fraudster that the bank could "block" this payment. The customer was also led to believe he needed to provide the OTP to the bank to confirm his identity (having already been through the bank's ID&V security questions) and to ensure that he was "not being hacked" (a vague explanation).

  Secondly, when the Bank's security challenged the attempted payment, the customer received a fraud prevention voicemail [redacted] *Having already been told by the fraudster that the OTP was required to "block" the payment, the customer was then also convinced that this* [redacted] *was required to 'block' the payment. Despite the voice message, he failed to call back on the prescribed Santander number;*

  Thirdly, the OTP made no reference to blocking a payment. The OTP is a dynamic code that forms part of the payment authorisation process. The customer provided this to the fraudster despite: (i) a clear and prominent warning not to share with anyone; (ii) his experience and historical use of the OTP in the payment process; and (iii) the OTP expressly referring to a "payment" rather than referring to blocking a payment;

  Finally, we disagree with the narrow view taken around the customer's failure to read and adhere to earlier warnings sent to him. There is a real risk of moral hazard if FOS's decision is perceived to condone customers' failure to comply with terms and conditions or to read and comply with in the moment and other warnings".

- Santander's view was that these factors, when taken in aggregate, considered objectively and taken together with the initial disclosure of personal security information, *"supported a conclusion that the customer fell well short of the standard of care to be expected of a reasonable person placed in the same circumstances."*

- In conclusion, Santander wished to make clear that its original decision to reject Mr B's complaint was *"based on assessment of all the relevant circumstances but specifically an objective assessment of what the customer actually did, against what he thought he was doing in the environment created by the fraudster, and set in the context of the in the moment and earlier warnings and relevant T&Cs."*

However, although Santander disagreed with a number of aspects of my provisional decision, it decided on balance to *"give the customer the benefit of the doubt and settle the matter".*

My understanding is that Mr B has now been compensated by Santander, in line with my provisional decision, for the fraud that there is no dispute he was a victim of.

my 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 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.

Relevant considerations

Santander as an FCA regulated firm provided a current 'deposit' account. As such the FCA's overarching principles for business apply including the requirement to 'Treat Customers Fairly'.

This fraud took place in March 2017, 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* (the PSRs 2009) which apply to transfers like the ones made from Mr B's account. Among other things the PSRs 2009 say:

"***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 transaction***

"*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 does not elaborate on what constitutes consent beyond saying that 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 the PSRs 2009 implement) does not explain what consent means here, but says "*In the absence of such consent, a payment transaction shall be considered to be unauthorised*." The Financial Conduct Authority's 2013 guidance on the PSRs 2009 also said nothing further about what consent means.

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 the PSRs 2009. However, 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.*"

A similar test existed historically through the Banking Code.

Negligence is often referred to as a failure to exercise reasonable care. So, I think it fair and reasonable to conclude (and I note the FCA expressed a similar view in its document), the use of 'g*ross negligence*', rather than mere 'negligence', suggests a level of recklessness, or lack of care, that goes significantly beyond ordinary negligence or carelessness.

the General Terms & Conditions of Mr B's account (March 2017)

The following extracts from the general terms and conditions of Mr B's current account are relevant to this case. These terms and conditions broadly reflect the provisions contained in the PSRs 2009.

"*7.2 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 from it and any fees and/or interest we may have charged in connection with the unauthorised payment. We will credit your account with lost interest that would have accrued on the amount of the unauthorised payment. We will not refund you if any of the circumstances listed in Condition 13.1 in Section 2A apply.

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.

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 was authorised by you or that any of the circumstances in Condition 13.1 in Section 2A apply.

"*9 Personal Security Details and protecting your account*

Summary: 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 …

"*9.1 We may provide you with Personal Security Details to enable you to access your account, using the internet, telephone and other remote access channels. We treat your use of your Personal Security Details as your consent to any instructions you give using the internet, telephone or other remote access channel …*

"*9.6 You must follow the safeguards to protect your chequebook, card, PIN and Personal Security Details set out in Condition 9.7 in Section 2A.*

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. To ensure this you must:

…

f) not disclose your PIN or Personal Security Details to anyone else, not even a member of Santander staff;

h) … (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 …

"*12.4 Where your card, passbook, PIN, or your Personal Security Details are used without your authority by someone else in circumstances other than those in Condition 12.3* [section 12.3 does not apply to this case] *in Section 2A then we may only debit up to £50 from your account. However, you will be responsible for the full amount of the transaction if any of the circumstances in Condition 13.1 in Section 2A apply.*

"*13 Responsibility for card, chequebook and remote access transactions*
Summary: this section explains circumstances where you are responsible for transactions on your account.

13.1 You are responsible for transactions from your account and any fees or interest incurred as a result of those transactions if:

a) you authorised the transaction;
b) someone else used your card, passbook, PIN or Personal Security Details with your agreement;
c) you deliberately, or with gross negligence, disclosed your PIN or Personal Security Details to someone else;
d) you deliberately failed to follow any of the safeguards referred to in Condition 9.7 in Section 2A or you are grossly negligent in failing to follow any of them;
e) you acted fraudulently;

f) after becoming aware you delayed unreasonably in notifying us that the transaction was unauthorised, incorrect or has not been carried out by us; or
g) you failed to tell us the transaction was unauthorised, incorrect or not carried out by us within 13 months of the date on which the transaction occurred or ought to have occurred.

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. If the law, or any code we subscribe to, limits your responsibility, we will not debit your account with more than that limit."

my thoughts on Santander's response to my provisional decision

Firstly, I'd like to thank Santander for promptly redressing Mr B for the fraud following my provisional decision.

Taking all the relevant considerations into account, including those set out above, I explained in my provisional decision that, in my view, there were two key questions that were particularly relevant to my consideration about what's fair and reasonable in Mr B's case.

1. Were the disputed transactions authorised by Mr B?

2. If they weren't, can the payment services provider demonstrate that Mr B acted with gross negligence – particularly taking into account the terms and conditions of his relationship with Santander and the obligations set out in Regulation 57 of the PSRs 2009?

Santander's response to my provisional decision did not dispute this. I will now deal the points that it has raised, broadly in the order that it raised them.

were the disputed transactions authorised by Mr B?

On the issue of the [redacted] call, I provisionally concluded, on balance, that I didn't think it was Mr B who responded to the [redacted] voicemail. I felt it was more likely than not to have been the fraudster. Santander has agreed that, if Mr B didn't make that call, he didn't authorise the payments in question and *"clear the payment".*

I also explained, in my provisional decision, that it was not possible, from the evidence I had seen, to say exactly what had happened here. And that I accepted there was a possibility that this call could have made by Mr B.

Ultimately, however, I was not persuaded, on the facts of the case, it more likely than not was Mr B. In reaching this view I took a number of things into account, including my view that, had Mr B been the person to make the call, there would have been a greater chance of this alerting him to something being amiss. And, therefore, for the fraudster to have suggested Mr B respond to the voicemail seemed to me, particularly taking into account Mr B's evidence about the step-by-step instructions and pre-emptions, to be introducing an element of 'risk' to the fraudster's chances of success, out of kilter with how he guided Mr B throughout the rest of this fraud – along with the sophistication of the fraud generally.

In reaching my provisional view on this issue, I thought a lot about the environment created by the fraudster for Mr B. I also thought about the fact we had asked Mr B for any itemised telephone bills he had from the time, but he was unable to provide one. I additionally took into account that we had checked and the telephone company Mr B uses does not

seemingly provide itemised telephone bills going back to when the fraud took place, unless Mr B had signed up to a particular paid service. Mr B confirmed that he was not signed up to that service at the time and I have no reason to disbelieve him.

I also gave Santander the opportunity, through my provisional decision, to provide any further evidence it might have that the [redacted] call was, in fact, made by Mr B. Santander, in effect, had the same opportunity when it carried out its own investigation prior to Mr B referring his complaint us. But no further evidence has been provided by Santander.

Taking all of the above into account, I don't agree that my investigation was incomplete on this point, or that it was unreasonable for me to proceed with my investigation based on the evidence that was available.

I remain of the view it was, more likely than not, the fraudster who made the [redacted] call and that for this reason, and the others detailed in my provisional decision, Mr B did not authorise the payments in dispute.

can the payment services provider demonstrate that Mr B acted with gross negligence – particularly taking into account the terms and conditions of his relationship with Santander and the obligations set out in Regulation 57 of the PSRs 2009?

Santander felt it was unclear, when assessing whether Mr B had been *"negligent to a degree which fell well short of the standard of care to be expected of a reasonable person, placed in the same circumstances"*, whether I had applied the 'objective reasonable person' test in my provisional decision. In reaching my conclusions about what is fair and reasonable in this case, and whether Mr B was grossly negligent, I have taken into account what a reasonable person might reasonably have been expected to have done in the circumstances. In reaching conclusions about gross negligence I particularly, but not exclusively, have thought about the following:

- As detailed in the relevant considerations section of this decision, the FCA, in its document setting out its role under the Payment Services Regulations 2017, said "*… 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.*"

- Mr B had no, or at the most very little, reason to suspect that the initial text message wasn't from Santander. It looked like it came through from a phone number that he'd previously received messages from Santander on - in fact it joined the same message thread. I think it would be fair to say that receiving a text message, that goes into the thread of previous conversations with the same 'contact', is very much an everyday occurrence for many, perhaps even most, people. So I can understand why it wouldn't, reasonably, have raised any obvious suspicion from Mr B – or any reasonable person in these circumstances. The environment created by the fraudster, which played such a part in Mr B's following actions, was perhaps first brought to life here.

- The plausibility of the original text message was increased in Mr B's eyes because it mentioned Apple and it was only a few days before that Mr B had signed up for Apple Pay. So there was little to make him wary about whom he was speaking with. But there was enough in the message to make him, or any reasonable person in the same circumstances, worried about a suspicious transaction, and anxious to protect

his money by following the instructions he was given. I think it's appropriate for his actions to be seen in that light.

- I appreciate Santander's point about Mr B giving the OTP code to the fraudster having already been through 'the bank's' security. However, to make too much of this, in the cold light of day, would, to my mind, significantly underplay the unrequested and stressful situation Mr B found himself in. Mr B was a victim of a sophisticated scam with social engineering at the very heart of it. So I don't think Mr B's choice here could reasonably be labelled gross negligence and/or at odds with the actions of a reasonable person.

- I have thought about Santander's responses in relation to Mr B not responding to the [redacted] call himself and the fact the OTP code made no reference to blocking a payment. My view on these points remains as stated in my provisional decision and for the same reasons. I don't think there is anything further I can usefully add to what I have said already on this.

- It is undoubtedly good practice for banks to send fraud warnings to customers. And as I said in my provisional decision, I appreciate raising public awareness of fraud is a big challenge for organisations like Santander. My role is to decide what is fair and reasonable in all the circumstances of a complaint – taking into account the relevant considerations. Specifically here, the question I have to decide is whether Mr B's failure to read the two particular warnings that were sent to his online banking account, something Santander's system was seemingly able to identify, amounted to gross negligence.

  For the same reasons that I gave in my provisional decision, I don't believe it, more likely than not, did.

  To be clear, in taking this position I'm not saying that fraud warnings by a bank aren't ever relevant at all, or couldn't, potentially, make a difference in a specific example of fraud. Nor am I condoning *"failure to comply with terms and conditions or to read and comply with in the moment and other warnings".* But by way of balance to this point, I also think it's right to appreciate and understand that, in a busy world, such emails are not always read by consumers and even if read may not, reasonably, be in a consumer's mind when faced with a sophisticated real time confidence trick of this nature some time later. It is encouraging to hear that banks are increasingly looking at ways to provide more 'real time' and impactful fraud specific warnings with this in mind.

  On the facts of this particular case, I don't believe Mr B's failure to read the warnings in question is enough, on the balance of evidence, for Santander to demonstrate gross negligence occurred here.

- I agree that a series of events, when taken together, can result in a 'tipping point' – which is essentially Santander's *"aggregate"* argument. I have thought about whether such a 'tipping point' can reasonably be said to have occurred in Mr B's case. However, I remain of the view that Mr B was the victim of sophisticated fraud, with social engineering at its heart, and that his actions, for the reasons I have said here and laid out in my provisional decision, do not amount to gross negligence – neither when taken in isolation nor in aggregate.

In conclusion, and as I touched upon in my provisional decision, cases such as Mr B's are a good example of the kind of finely balanced decisions I have to make in circumstances where none of us can know, for sure, everything that has occurred with certainty. But Mr B has painted a compelling and plausible picture which has led me to find that he has not acted in a grossly negligent manner– which I believe is on balance supported by the evidence when taken as a whole.

Businesses of course have a similar challenge to our own – not least in this area where frauds are becoming increasingly sophisticated, fraudster's have become so adept at social engineering and the impact on their customers can be so significant – both financially and emotionally.

I accept that Santander's original decision to reject Mr B's complaint was based on what it believed was an objective assessment of the facts – as it described in its response to my provisional decision. But I have a different view of what a fair and reasonable outcome would be in Mr B's case – for all the reasons I have said both here and in my provisional decision.

my final decision

My final decision is that I uphold Mr B's complaint.

As I mentioned earlier in this decision, Mr B accepted my provisional decision and I believe Santander has compensated Mr B in line with it. But for the sake of completeness:

- To put things right for Mr B, Santander UK Plc should, if it has not already, refund the remaining balance that he has lost; £12,275.29, adding interest from the date of the disputed transactions to the date of settlement at the rate Mr B would have received had the money remained in his 1-2-3 account. If Santander deducts tax from the interest element of this award, it should provide Mr B with the appropriate tax deduction certificate.

- In deciding what is fair compensation, I have taken into account the terms and conditions of Mr B's account – in particular condition 7.2(a) and I have assumed that had the fraudster not taken the money, it would have remained in Mr B's account.

- In making this refund Santander, in accordance with the terms and conditions applicable to Mr B's account, are entitled to withhold up to £50 (paragraph 12.4). If it exercises this right, I consider that it would be fair and reasonable for it to inform Mr B of its decision to do so.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 16 September 2018.

Patrick Hurley
ombudsman

copy of my provisional decision

complaint

Mr B complains that Santander UK Plc won't refund £12,310 of payments from his account that he says he didn't authorise.

background

Mr B held a 1-2-3 current account with Santander. In March 2017 he was the victim of a scam known as "*smishing*" (this is where a fraudster sends an SMS text message to a customer and it appears to come from their bank). It is not in dispute that what happened to Mr B was an act of fraud, so I have used the term "*fraudster*" throughout to refer to the third party involved.

Mr B says that, on 2 March 2017, he received a text message which appeared to come from Santander. The message looked like it had been sent from the same phone number that he'd previously received messages from Santander on. The message came up on his phone as being from 'Santander' and joined the Santander 'message thread' – alongside the messages he had genuinely received from the bank. He therefore assumed that the message had in fact been sent by Santander. The message read:

"*Santander has noticed your debit card was recently used on 02-03-2017 15:59:03 at APPLE ONLINE STORE for 1,976.00 GBP. If not you please urgently call fraud prevention on XXXXXXXXXXX or Intl XXXXXXXXXXX. Do not reply by SMS*".

Mr B had recently signed up for 'Apple Pay' (a system allowing a consumer to use their phone, rather than their physical debit or credit card, to make purchases). He thought the message might be connected to that. As he didn't recognise this transaction, he called the "*fraud prevention*" number given and was asked a series of questions.

Mr B can't recall exactly what questions he was asked, or what answers he gave to those questions. Mr B's recollection of this interaction is that they *"went through the normal security etc. and worked through the issue of the Apple payment".* It seems that whilst talking to Mr B, the fraudster accessed Mr B's online banking facility and through that his account.

Whilst in Mr B's online account, the fraudster changed the account details for one of Mr B's existing payees. The fraudster changed the details to such an extent that it altered the account number and sort code of an existing bill payment.

Mr B, who says he was still on the telephone to the fraudster at this point, then received a One Time Passcode (OTP) message to his phone from Santander. Mr B says the fraudster pre-empted the receipt of this message by telling him he would receive the code shortly, via text message. Mr B says that the fraudster told him that he would need to *"know the OTP"* in order to clarify it was Mr B on the phone and that he was *"not being hacked".* And that in doing this, it would stop the Apple payment. Mr B recalls that *"as soon as he said this the text came through".*

The OTP message arrived in the same thread as the original message from the fraudster and the genuine text messages that Mr B had previously received from Santander. In view of this, Mr B said it *"rose no alarm bells"* for him.

The message 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 XXXXXXXX*".

Mr B gave the code to the fraudster and, shortly afterwards, £12,300, along with a second payment of £10.00, was transferred out of his account to the newly 'amended' payee.

Mr B was still on the telephone to the fraudster when Santander sent him an automated fraud prevention voicemail (known as an [redacted] call) asking him to call them back. Mr B says that the fraudster, once again, pre-empted this by telling him that he was going to send the voicemail to him. Mr B's recollection of this is *"as soon as he finished saying the words my phone buzzed".*

The voicemail contained the following:

[redacted]

Mr B says that the fraudster asked him to listen to the voicemail and to give him the *"information"* contained within it. He said that he did as instructed because the fraudster told him the information was necessary to stop the suspicious payment. Mr B added that *"because of the nature of the text message and official voicemail, I had no reason to think otherwise".*

The following afternoon, on 3 March 2017, a member of staff from Santander's fraud and security team called Mr B to ask him whether he had made the transactions for £12,310. They left him a voicemail asking him to call back. When he did so and confirmed that he hadn't authorised the transactions, a fraud investigation began.

Santander was only able to recover £35 from the recipient bank - it says the money was moved very quickly and used to buy foreign currency. It refused to reimburse Mr B the rest as it was satisfied that he'd authorised the disputed payment by using the OTP. It also explained that Mr B had responded to the [redacted] call, on 2 March 2017, confirming via its automated system that he recognised the transactions.

Santander has provided the following transcript of what happened when the [redacted] call was responded to:

[redacted]

Mr B has no recollection of responding to a voicemail from Santander until 3 March 2017. This is when he called Santander back, in response to the message left by a member of staff (not an automated message), and spoke with someone in the fraud and security team.

Specifically, Mr B does not remember replying to an automated voicemail on 2 March 2017 – other than to provide the fraudster with the *"information"* contained within it as instructed. Mr B has been clear that he does not remember responding to any automated questions about the transactions using his phone key pad. On this, he has said *"I do not remember that call at all".*

For clarity, this appears to be the approximate timeline of what happened on 2 March 2017:

16:07	Mr B received a text message which looked like it had come from Santander
16:11	The fraudster logged on to Mr B's online banking
16:17	Mr B received an OTP by text message
16:19	Payment made to amended payee for £12,300
16:20	call attempted, voicemail left for Mr B, followed shortly by unsuccessful inbound call
16:40	Payment made to amended payee for £10.00, followed shortly by unsuccessful inbound call
16:46	Someone responded to the voicemail confirming transactions as genuine
16:48	The fraudster logged off from Mr B's online banking

In its final response to Mr B's complaint, Santander said that it makes significant efforts to educate customers about potential scams. And that its message to customers is that they should never disclose their security details. Santander also said it had sent two emails to Mr B, informing him about the threat of "*smishing*" scams in November 2016 and January 2017, but that he had not read them.

In respect of the [redacted] calls, Santander said the following to Mr B:

"At 16:20, our Automated Fraud Monitoring System attempted to contact you to validate this payment as genuine, however they were unable to get through on your registered mobile. At 16:40, the fraudster made a further payment for £10.00 to the same destination account. At 16:40, we tried to make further contact with you to authorise the payment, but the line was disconnected.

These contacts were made after your registered number satisfied our internal SIM swap checks. At 16:46 we then received confirmation via our Automated Fraud Monitoring System that the Bill Payment was genuine. However, had the OTP not been provided, the transactions would not have debited."

my provisional findings

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

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 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.

Relevant considerations

Santander as an FCA regulated firm provided a current 'deposit' account. As such the FCA's overarching principles for business apply including the requirement to 'Treat Customers Fairly'.

This fraud took place in March 2017, 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* (the PSRs 2009) which apply to transfers like the ones made from Mr B's account. Among other things the PSRs 2009 say:

"***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—*

(c) use the payment instrument in accordance with the terms and conditions governing its issue and use; and

(d) 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—*

(c) denies having authorised an executed payment transaction; or

(d) 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 transaction***

"*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 does not elaborate on what constitutes consent beyond saying that 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 the PSRs 2009 implement) does not explain what consent means here, but says "*In the absence of such consent, a payment transaction shall be considered to be unauthorised*."
The Financial Conduct Authority's 2013 guidance on the PSRs 2009 also said nothing further about what consent means.

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 the PSRs 2009. However, 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.*"

A similar test existed historically through the Banking Code.

Negligence is often referred to as a failure to exercise reasonable care. So, I think it fair and reasonable to conclude (and I note the FCA expressed a similar view in its document), the use of 'g*ross negligence*', rather than mere 'negligence', suggests a level of recklessness, or lack of care, that goes significantly beyond ordinary negligence or carelessness.

the General Terms & Conditions of Mr B's account (March 2017)

The following extracts from the general terms and conditions of Mr B's current account are relevant to this case. These terms and conditions broadly reflect the provisions contained in the PSRs 2009.

"*7.2 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 from it and any fees and/or interest we may have charged in connection with the unauthorised payment. We will credit your account with lost interest that would have accrued on the amount of the unauthorised payment. We will not refund you if any of the circumstances listed in Condition 13.1 in Section 2A apply.

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.

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 was authorised by you or that any of the circumstances in Condition 13.1 in Section 2A apply.

"*9 Personal Security Details and protecting your account*

Summary: 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 …

"*9.1 We may provide you with Personal Security Details to enable you to access your account, using the internet, telephone and other remote access channels. We treat your use of your Personal*

Security Details as your consent to any instructions you give using the internet, telephone or other remote access channel …

"*9.6 You must follow the safeguards to protect your chequebook, card, PIN and Personal Security Details set out in Condition 9.7 in Section 2A.*

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. To ensure this you must:

…

f) not disclose your PIN or Personal Security Details to anyone else, not even a member of Santander staff;

h) … (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 …

"*12.4 Where your card, passbook, PIN, or your Personal Security Details are used without your authority by someone else in circumstances other than those in Condition 12.3* [section 12.3 does not apply to this case] *in Section 2A then we may only debit up to £50 from your account. However, you will be responsible for the full amount of the transaction if any of the circumstances in Condition 13.1 in Section 2A apply.*

"*13 Responsibility for card, chequebook and remote access transactions*
Summary: this section explains circumstances where you are responsible for transactions on your account.

13.1 You are responsible for transactions from your account and any fees or interest incurred as a result of those transactions if:

a) you authorised the transaction;
b) someone else used your card, passbook, PIN or Personal Security Details with your agreement;
c) you deliberately, or with gross negligence, disclosed your PIN or Personal Security Details to someone else;
d) you deliberately failed to follow any of the safeguards referred to in Condition 9.7 in Section 2A or you are grossly negligent in failing to follow any of them;
e) you acted fraudulently;
f) after becoming aware you delayed unreasonably in notifying us that the transaction was unauthorised, incorrect or has not been carried out by us; or
g) you failed to tell us the transaction was unauthorised, incorrect or not carried out by us within 13 months of the date on which the transaction occurred or ought to have occurred.

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. If the law, or any code we subscribe to, limits your responsibility, we will not debit your account with more than that limit."

key questions

Taking all the relevant considerations into account, including those set out above, I think there are two questions that are particularly relevant to my consideration about what's fair and reasonable here.

1. Were the disputed transactions authorised by Mr B?

2. If they weren't, can the payment services provider demonstrate that Mr B acted with gross negligence – particularly taking into account the terms and conditions of his relationship with Santander and the obligations set out in Regulation 57 of the PSRs 2009?

Though there is naturally some overlap of events when answering these two questions, I will approach them in this order.

were the disputed transactions authorised by Mr B?

Although Santander says that Mr B authorised the disputed payments, on the balance of evidence, I don't agree.

It's important to remember, when considering each aspect of this matter, the environment created by the fraudster for Mr B. This began at first contact – a text message received in the Santander message thread he was familiar with and trusted.

I acknowledge that, although Mr B does not recall what answers he gave to the fraudster's questions, when he responded to the initial message and thought he was going through *"security"* with Santander, he probably divulged enough information - along with perhaps anything the fraudster was able to socially engineer - to allow the fraudster to log-on to his online banking. There is currently no other explanation, at least not one that I am presently aware of, for how the fraudster managed to achieve this. Santander has said the fraudster would have to have known Mr B's personal ID number, partial password and partial online banking PIN.

Of course, had Mr B been actually speaking to the bank, as he thought he was – in what I can appreciate would have been a worrying and time sensitive situation for him - it would have asked him a number of security questions and this would also have meant providing security information. So I can understand why Mr B refers to this as being like going through *"security".*

Mr B also gave the fraudster the OTP to amend a payee. This action on Mr B's part was a major step in the process which allowed the payment transactions to be made. However, at no time during the call with the fraudster, did Mr B know that any payment transactions were going to be made from his account (regardless of who to). Nothing in the wording of the message Mr B received containing the OTP, as far as I can see, suggested it could, or would, be used to authorise a transaction.

So I don't think it can fairly and reasonably be said that by potentially divulging his log-in details, along with the OTP code, Mr B authorised the transactions. And for the purposes of condition 9.1 of the account terms and conditions, it was the fraudster, not Mr B, using his personal security details.

The actions the fraudster then took, when armed with the OTP code, in my view, went beyond what I expect many people might reasonably imagine by the word 'amend' – the result of these actions was, in effect, a 'new' payment to someone Mr B had never made a payment to before. But, either way, as I have discussed above, Mr B didn't know what payment would be made and he didn't himself input those details into his online banking screen - the fraudster did. So his 'mistake' was handing over the code to the fraudster to enable the fraudster to authorise the transactions. Mr B was oblivious and not complicit and I don't therefore think it can fairly and reasonably be said he authorised it. In fact, Mr B thought he was 'sharing' the code with his bank to prevent a transaction. Whether he was grossly negligent in doing this, I will come to later.

Santander has relied heavily on Mr B's response to the [redacted] call as evidence that he knew about the payments and confirmed them as genuine before the money left his account.

It's not possible, from the evidence I have seen, to say exactly what happened here and the question of who did, or didn't make this call, is a good example of the kind of finely balanced decisions I have

to make in circumstances where I cannot know for sure what has occurred – decisions that I must make on the balance of evidence fairly and reasonably.

I've decided, on the balance of evidence I've seen, that I don't think it was Mr B who responded to the [redacted] voicemail. I think it's more likely than not to have been the fraudster.

Mr B has said that, in following the instructions he was being given by the fraudster during the telephone conversation, he gave the *"information"* he received in the voicemail over to the fraudster. This would have included the [redacted] But he has no recollection of making another call or responding to any automated questions about the transactions using his phone key pad.

In case it could help shed any further light on what happened, we have asked Mr B for any itemised telephone bills he has from the time. He's been unable to provide one. Additionally, we have checked and the telephone company Mr B uses does not provide itemised telephone bills going back that far.

I cannot say for sure what happened here. And I accept there is a possibility that this call was made by Mr B, but I am not currently persuaded this was more likely than not. If Santander can provide evidence that shows this call was in fact made by Mr B, I would naturally reconsider my findings in light of that. However, having carefully considered the circumstances and the evidence available to me, I think the most likely scenario is Mr B, who was of course being talked through every step of the process by the fraudster, followed the fraudster's instructions [redacted]

I think Mr B did this because the fraudster had created a plausible environment, from the initial text message to the step-by-step pre-emptions, which made this a quite normal and not unreasonable in the circumstances thing for Mr B to do. The fraudster then armed with this information, called the automated [redacted] service at 16:46.

Had Mr B been the person to make the call, there would have been a greater chance of this alerting him to something being amiss. And for the fraudster to have suggested Mr B respond to the voicemail would seem to me, particularly taking into account Mr B's evidence about the step-by-step instructions and pre-emptions, to be introducing an element of 'risk' to the fraudster's chances of success out of kilter with how he guided Mr B throughout the rest of this fraud and the sophistication of the fraud generally.

So I don't think, on the balance of evidence I've seen, Mr B was the person who responded to the [redacted] call. I think it's more likely the fraudster had convinced him that he was already speaking with a member of the "*fraud department*", and that all Mr B needed to do was relay to him the [redacted] Whether this amounts to gross negligence, I will discuss when answering that question shortly.

In summary, whilst I acknowledge that Mr B, under the instruction of a fraudster who he genuinely believed to be from Santander, took some steps which made it possible for the fraudster to make the payment transactions, I don't think Mr B gave his consent to them. Based on the available evidence, I'm also satisfied that the call responding to the [redacted] call voicemail, during which someone confirmed the transactions as genuine, is more likely to have been completed by the fraudster, not Mr B.

In these circumstances, I don't think it would be fair or reasonable to say that Mr B authorised the transactions.

My starting point, therefore, is that it would not be fair and reasonable for Mr B to be held liable for these transactions – which I think are more likely than not to have been unauthorised - unless he has failed with intent or gross negligence to comply with the terms and conditions of his relationship with Santander and the obligations set out in the PSRs 2009.

can the payment services provider demonstrate that Mr B acted with gross negligence – particularly taking into account the terms and conditions of his relationship with Santander and the obligations set out in Regulation 57 of the PSRs 2009?

The principal obligation relevant to this case is the obligation on Mr B to take all reasonable steps to keep the personalised security features of his account safe. The terms and conditions of Mr B's account that relate to this obligation, detailed earlier in this provisional decision, show, amongst other things, how Santander expect this to play out in practice and I have considered them carefully.

Unfortunately, its likely Mr B was initially tricked into divulging to the fraudster enough details, at least partially, to allow him access to his online banking. He was also tricked into providing an OTP, which allowed the fraudster to change the sort code and account number of an existing payee. He was also, in my view, tricked into providing a [redacted] which allowed the fraudster to make it look like Mr B had confirmed the subsequent transactions as genuine.

However, I don't, on the balance of evidence, think it would be fair and reasonable to say that Mr B was grossly negligent when he divulged this information in the circumstances he did.

As I've said earlier in this provisional decision, negligence is often referred to as a failure to exercise reasonable care. So, and as touched upon in the FCA's document, the use of '*gross negligence*', rather than mere 'negligence', suggests a level of recklessness, or lack of care, that goes significantly beyond ordinary negligence or carelessness.

Gross negligence is not an abstract concept. It's obviously important to take into account all the circumstances when considering whether an individual's actions amount to gross negligence. I believe the scenario the fraudster created was particularly convincing. I consider this for a number of reasons.

Mr B had no, or at the most very little, reason to suspect that the initial text message wasn't from Santander. It looked like it came through from a phone number that he'd previously received messages from Santander on - in fact it joined the same message thread. I think it would be fair to say that receiving a text message, that goes into the thread of previous conversations with the same 'contact', is very much an everyday occurrence for many, perhaps even most, people. So I can understand why it wouldn't, reasonably, have raised any obvious suspicion from Mr B.

The plausibility of the message was increased in Mr B's eyes because it mentioned Apple and it was only a few days before that Mr B had signed up for Apple Pay. So there was little to make him wary about whom he was speaking with. But there was enough in the message to make him worried about a suspicious transaction, and anxious to protect his money. And I think his actions must be seen in that light.

I have thought about the fact that Santander sent periodic warnings to Mr B about "*smishing*" scams, and I acknowledge that it's good practice to send such warnings, with consumer protection in mind. Increased levels of consumer awareness may in some cases help to prevent frauds like this from succeeding. But I also appreciate that such emails are not always read by consumers and even if read may not, reasonably, be in a consumer's mind when faced with a sophisticated real time confidence trick of this nature some time later. Santander has said Mr B did not read the warnings it sent him. However, I do not think that, in failing to read these particular warnings, it would be fair and reasonable to say Mr B was grossly negligent – either on this specific issue or taking into account the circumstances of this case as a whole. I appreciate that increasing the public awareness of fraud is a big challenge for businesses.

Mr B genuinely believed that he was talking to a member of staff in Santander's "*fraud prevention*" team and was unaware that the security features of his online banking account weren't safe at this stage. He felt the initial questions the fraudster asked were the type of *"security"* questions that a bank will of course always ask a selection of when contacted by a customer. The wording of the OTP text which then came through during this call fitted with what the fraudster was telling him – quite literally, in this case, because the evidence suggests Mr B was reading the message with the fraudster still on the telephone walking him through it. The message referred to amending a payee. I don't think, in the

environment the fraudster created, it's unreasonable that Mr B thought this related to stopping the suspicious payment going out, rather than a payment to someone new.

The OTP message included the words, "*Don't share this code with anyone*". In the context of Mr B's genuine belief that he was speaking with Santander staff, I can't say that his failure to pay closer attention to this wording was more than careless. He wasn't in my view behaving recklessly in the face of a risk he appreciated, he was acting under the belief that his money was at risk and that the person he was speaking with, from his bank, was helping him protect his account. I therefore don't think in the circumstances of Mr B's case that this could fairly and reasonably be said to amount to gross negligence.

Finally, the fraudster anticipated that Mr B would receive the voicemail and I don't find it surprising that Mr B was persuaded to give him the After all, Mr B believed he was already speaking with the fraud department and the voicemail had told him I can see how the environment created by the fraudster, along with the time pressure of how this unfolded, could have 'normalised' this situation for Mr B. His actions could perhaps be described as careless at the most. But, again, I don't think in the circumstances of Mr B's case that this could therefore fairly be called gross negligence.

So, although Mr B was persuaded to divulge security features to a fraudster as part of a sophisticated and successful scam, and on more than one occasion, I'm not currently minded to find that Santander has demonstrated Mr B's actions amounted to gross negligence.

my provisional decision

As I touched upon before, cases such as Mr B's are a good example of the kind of finely balanced decisions I have to make in circumstances where I cannot know for sure everything that has occurred – decisions that I must make on the balance of evidence fairly and reasonably. Businesses of course have a similar challenge – not least in this area where frauds are becoming increasingly sophisticated and the impact on their customers can be so significant.

However, for all the reasons I've said above, I think it's fair and reasonable to ask Santander to reimburse Mr B's loss.

My provisional decision is that I am minded to uphold this complaint. To put things right for Mr B, I propose that Santander UK Plc refunds the remaining balance that he has lost; £12,275.29, adding interest from the date of the disputed transactions to the date of settlement at the rate Mr B would have received had the money remained in his 1-2-3 account. If Santander deducts tax from the interest element of this award, it should provide Mr B with the appropriate tax deduction certificate.

In reaching my provisional conclusions about what is fair compensation, I have taken into account the terms and conditions of Mr B's account – in particular condition 7.2(a) and I have assumed that had the fraudster not taken the money, it would have remained in Mr B's account. But I would invite the parties to make further representations about this if they have a different view.

In making this refund Santander, in accordance with the terms and conditions applicable to Mr B's account, are entitled to withhold up to £50 (paragraph 12.4). If it exercises this right, I consider that it would be fair and reasonable for it to inform Mr B of its decision to do so.

Patrick Hurley
Ombudsman