complaint

Mr and Mrs B complain that Santander UK Plc won't refund a £15,000 payment made from their account that they say they didn't authorise.

background

Mr and Mrs B held a 1-2-3 current account with Santander. In February 2017 Mr B 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).

Mr B says that, on 27 February 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' – following 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 27-02-2017 18:23:03 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 says that he was confident that when he rang the number shown on the text he was speaking to a member of staff from Santander to resolve the problem. And this was the reason he passed on his details to the female he was speaking with. He says he was confident the person he was speaking to was dealing with the problem of someone using his details to make a payment on his account. Mr B says he also had a similar problem with his bank account in March 2016 and had to close his account and open a new one (with Santander) and was assured it would be flagged when there were any future similar attempts to remove funds from his account.

Mr B hasn't said what questions he was asked, or what answers he gave to those questions. Mr B is saying he didn't log into his online banking. It seems that whilst talking to Mr B, the fraudster accessed Mr B's online banking facility using information that they managed to convince Mr B to share with them, and through that accessed his account. Santander says that in order to access Mr and Mrs B's joint account the fraudster would've needed "the log on number, date of birth and parts of Mr B's security number". Santander says because a new IP address was used to log in to Mr B's online banking an additional security question was required and passed. Mr B confirms he was asked to provide his place of birth to the caller – which Santander believes is likely to be the additional security question asked at this stage.

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, effectively creating a new payee. This action prompted a One Time Passcode (OPT) to be sent from Santander to Mr B's mobile phone to verify the change.

Mr B, who says he was still on the telephone to the fraudster at this point, then received a text message containing an OTP to his phone.

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. 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, he thought to protect his account and, shortly afterwards, £15,000, was transferred out of this joint account to the newly 'amended' payee.

Santander's security system flagged the payment out of the account and this prompted another layer of security. This was an automated call to Mr B providing a three digit security code that he would need to call back and provide to Santander to confirm the payment as genuine. Its systems detected a SIM change on Mr B's phone so didn't use the mobile number to make the security call. But Santander's system attempted to call Mr and Mrs B's home phone number 28 times and then left an automated voicemail with the three digit security code. Mr B confirms he listened to the voicemail and, under the fraudster's instruction, gave this code to them, and that doesn't appear to be in dispute.

Someone then called Santander's automated system entering the three digit code, and confirming the payment from Mr and Mrs B's account as genuine.

Below is a table of key events:

18:23	Mr B received a text message which looked like it had come from Santander and Mr B called the number and gave over enough security information during the call to enable the fraudster to access Mr B's online banking.
18:40	The fraudster logged onto Mr B's online banking.
18:41	Mr B received an OTP by text message from Santander.
18:44	The OTP was input to amend payee (mandate 9). A payment for £15,000 was made out of the account to the newly amended payee.
18:45	Santander's security system tried to contact Mr B – mobile number checked and SIM changed from last contact so no call made to mobile. 28 attempts made to contact Mr and Mrs B's home number – Santander's notes say "*no response block applied to system*".
18:47	Santander's security system called landline – automated voicemail message left containing three digit security number needed to call back Santander to allow payment to proceed.
18:50	Mr B says he gave that code to the fraudster and someone then responded to automated security call providing the three digit code confirming the transaction as genuine and the payment was made from Mr and Mrs B's account
19:40	Mr B called Santander after receiving a text to say his account was overdrawn by £335.10. He asked about earlier conversation to a prevent payment and then discovered this had been a scam

Mr B reported the scam at 19.40 on 27 February 2017. This was 50 minutes after the monies had been sent. Santander says the recipient bank could not be contacted that night. It says it contacted the recipient bank at 8.38am on 28 February 2017. Santander says this seems a reasonable action as the scam was reported outside of normal working hours.

The receiving bank has confirmed the money left the account at on 27 February at 20:07.

Mr B is unhappy that Santander didn't warn him and other customers that fraudsters were targeting people with this particular type of scam. In particular Mr B feels that Santander should have warned him about the "*smishing*" text messages that were being sent to consumers.

In response to this Santander has said:

The issue of texts attaching themselves to a specific genuine text thread is part of the way SMART phones are set up. It is the fraudsters who are using an app that makes it appear a text message is coming from Santander's number. We have no control over this. When received the message attaches itself to an existing thread on the recipient phone from that number. There is no evidence of Santander error.

Santander has tried to educate customers to scams by the following means

1. *Electronic messages sent via online banking mailbox. Mr B has received messages on 11 January 2017 and 22 November 2016 giving security advice on scams both of which show as having been read. The message on 11 January 2017 specifically warns about receiving spoofing texts although it does not mention that text messages can attach themselves to previous threads on the phone.*

2. *A message on the home internet ''sign on'' page specifically advises never to disclose or enter an OTP following an instruction from a third party.*

3. *Branch leaflets giving specific fraud advice.*

4. *Customer call centre message providing advice on how to avoid fraud although not specifically mentioning spoofing.*

5. *Statement insert issued with Dec 14 statements. This advised customers not to divulge security information to any third party specifically highlighting OTPs and stating Santander will never ask for an OTP by phone contact.*

Santander says its email message sent to Mr B''s online banking mailbox on 11 January 2017 said:

Never rely on caller ID alone to authenticate a caller or a text message. Criminals can ''spoof'' caller ID numbers, meaning you can't be sure the number displayed on your phone belongs to the company it claims to be from.

my provisional decision

On 07 December 2018 I issued a provisional decision on Mr and Mrs 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, plus interest at the rate he would have received had the money remained in Mr and Mrs B's joint account; and
- Santander should pay Mr and Mrs B £300 for the trouble and upset they experienced.

Mr and Mrs B responded to say they accepted the findings set out in my provisional decision.

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

my findings

I've re-considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint. As both parties accept my provisional findings I see no reason to depart from these.

For clarity I've set out the relevant considerations here and a summary of the findings in my provisional decision as well and my directions to Santander to put the matter right.

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 B''s account were made in February 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 (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 Mr B did fell so far below the standard expected of a reasonable person that it would be fair to say he failed with gross negligence to keep his personalised security details safe or to comply with the Terms and Conditions of the account.

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

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

6. "*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 says *"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 provisional 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 B unless Mr B, with intent or gross negligence, failed to comply with the Terms and Conditions of the account and the obligations set out in Regulation 57.

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 Mr B? and;

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

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?

All parties agreed that Mr B did not authorise this transaction. When he received the OTP from Santander he gave this the fraudster and they entered this into online banking in order to process a payment from Mr and Mrs B's joint account, Mr B did not consent for any money to leave his account. I was also satisfied that Mr B did not call back Santander and provide the three digit security that it left for him in a voicemail, again he passed this information to the fraudster and they used it to verify the payment.

So, my starting point here is that it wouldn't be fair and reasonable for Mr B to be held liable for the transaction – which I think is 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 the relationship with Santander and the obligations set out in the PSR 2009.

did Mr B fail with gross negligence either to comply with the Terms and Conditions of the account, or to keep his personalised security details safe?

In my provisional decision I also concluded that I didn't think Mr B had been grossly negligent. I concluded that Mr B was tricked by a fraudster into giving over some account security information. Mr B was also then tricked into handing over an OTP which allowed an existing payee to be amended, effectively making it into an entirely new payee. And he was tricked into giving over the three digit security code he received in an automated voicemail from Santander. However, on the balance of evidence, I don't currently think it would be fair and reasonable to say that, in falling for these tricks and failing to keep his security details safe, Mr B was grossly negligent.

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 Mr B took in the circumstances here, and whether what he did, fell so far below the standard of a reasonable person that it would be fair to say he failed with gross negligence to keep his 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 *"smishing*" and "*social engineering*", where fraudsters use a range of sophisticated techniques to trick, deceive and manipulate their victims into giving out confidential information. Here Mr B was made to believe he was talking to his own bank, needing to act quickly to protect his bank account which was currently being used for fraudulent spending. So I've thought about Mr B''s actions in that context, and considered his actions overall.

I have seen the text message Mr B received and he has described how it followed other genuine text messages from Santander. He said it looked genuine and I don't doubt his account of this. This is a sophisticated method used by fraudsters to trick their victims into a sense of security, and into believing that they are dealing with their genuine bank and that they need to act quickly to protect their account. So I can understand why it wouldn't, reasonably, have raised any suspicion from Mr B – or any reasonable person in these circumstances.

I don't think, at the time, Mr B thought the actions he was taking were for any other purpose than to prevent a fraudulent payment leaving his account, and to secure his bank account. Rather than appreciating the risk he was taking by following the fraudsters instructions, but disregarding or being indifferent to it, he was under the opposite impression - that if he didn't follow those instructions he was at risk of losing his money.

Mr B hasn't been able to provide us with much detail about what the fraudster told him the OTP and three digit code were for. But from what he has said, I think it likely the fraudsters convinced him the codes were needed in the process of protecting his money and the various stages the bank needed to go through to do that. And I wouldn't expect Mr B to know what Santander's processes are for stopping a payment, or to necessarily question what he was being asked to do, because he genuinely believed he was working with his bank to protect his account. He'd also been on the telephone to the fraudster for some time and was worried about the security of his bank account, and felt pressure to act. In similar circumstances I think many people would've acted in the same way that Mr B did here.

So on balance I'm not currently persuaded that his actions fell so far below what a reasonable person would do in the circumstances to amount to gross negligence.

warnings

I also mentioned the warnings Santander says it sent to Mr B prior to the fraud. But on the facts of this particular case, I don't believe Mr B's failure to read or head the warnings in question is enough, on the balance of evidence, for Santander to demonstrate gross negligence occurred here.

putting things right

As both parties agree, I now direct Santander to:

- refund Mr and Mrs B's joint account with £15,000; 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 B with the appropriate tax deduction certificate.

- this has been a very worrying time for Mr and Mrs B. Having considered the matter as a whole and the concern it caused Mr and Mrs B, being told they wouldn't receive a refund of such a large amount of money, I think it would be fair for Santander to pay Mr and Mrs B 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 B responsible for the first £50 of their loss. If it intends to do this, it can take this amount from the £15,000 before adding the interest element.

my final decision

As I've concluded above I now direct Santander UK plc to settle Mr and Mrs B's complaint as I've set out both here and in my provisional decision.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr and Mrs B to accept or reject my decision before 1 March 2019.

Sophia Smith
ombudsman