complaint

Mr M is unhappy with Santander UK Plc's decision not to refund money taken from his account as part of a scam.

background

In setting out the background to this complaint I think it's worth stating that all parties accept that Mr M has been the victim of a cruel scam and that a malicious third party (or parties) has been involved. With that in mind I will refer to some of the actions and events as being carried out by 'the fraudster'.

Mr M received a text message on 1 March 2017 and it appeared to be from Santander. It was in the same chain of genuine texts he'd received from the bank in the past. But it hadn't actually been sent by Santander. Instead, a fraudster had used a known method to 'spoof' the name of the sender. That's to say that although the text was sent from a different number, it appeared as though it was sent by Santander. It's also sometimes referred to as 'smishing'. The text said:

*Santander has noticed your debit card was recently used on 01-03-201716:26:43, at APPLE ONLINE STORE for 1976.00 GBP. If not you please urgently call fraud prevention on 03********* or Intl +443********* . Do not reply by SMS*

Mr M hadn't tried to make the transaction referred to and, believing the text was genuinely from the bank, he called the number in the text message. He was concerned someone was trying to steal his money. But it wasn't a genuine Santander number and instead Mr M was calling the fraudster.

The call was answered and the person Mr M spoke with took him through security. Mr M recalls how it seemed just like any other genuine call he'd had with Santander in the past. He remembers answering security questions which included giving, among other things, his customer ID. He's unsure about what characters, if any, he gave from his online banking password. But he knows there were also questions about his date of birth along with other personal information.

Mr M recalls getting straight through to the fraudster and that once security was passed they assured him they could help. Mr M was told the payment could be stopped from going through and that a new card would be sent to him. He believed he was speaking with the bank and that someone was helping him. He's described to us how he went from panicking about someone trying to use his card to thinking the bank was helping him, all within a few minutes.

Mr M, in his later recollections, thinks the person he was speaking to may have also taken him through the steps necessary to set up call forwarding on his phone. He remembers following some instructions which included adding another caller to the conversation and entering a string of digits which he thinks may have been a phone number.

Mr M's online banking was then accessed by fraudsters most likely using the personal information and details they'd gathered from Mr M whilst talking him through 'security'. Mr M has said it wasn't him logging in and that it must have been the fraudster. He had no idea this was happening whilst he was on the call with the fraudster. One of the existing payees

on Mr M's online banking was amended; the recipient account number and sort code were changed at 16:58.

Mr M then received a text from Santander. This was a genuine text, received in the same thread as earlier genuine texts and the fraudulent ones sent on the day, and it contained a one-time passcode (OTP). That OTP was used to confirm the changes that had just been made to the payee through online banking. The text message said:

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.

Mr M has said he doesn't remember seeing this OTP on the day. He's quite certain he didn't give it to the fraudster. But it seems that it was entered online somehow as the payee was successfully amended. Santander has said the only way for that to happen would be for someone to correctly enter the OTP online. Mr M's certainty of not handing over the OTP is one of the reasons he thinks there was some kind of call forwarding established.

A payment was then set up online for a total of £9,182.17 at 17:05. Mr M has said he didn't do this himself or otherwise authorise for it to happen. Santander flagged this transaction as suspicious and stopped it from leaving the account. It then made an automated security call to Mr M's landline. It appears there was an attempt to reach the mobile phone as the system conducted a check against Mr M's sim card which came back as a match. But Santander has confirmed the actual call went to Mr M's landline.

An answering machine picked up the call and a message was left in which Mr M was given a three digit code. The code was needed to release the payment that had been set up online. The message gave a phone number for Mr M to call in order to give over the code. But there was no mention of what the code was for specifically; it didn't mention a payment was being made out of the account.

I can see from Santander's records that there are then several calls to it where attempts are made to verify the payment. Each is listed as "call disconnected while trying to confirm details". These calls run from 17:13 until 19:02 but it's unclear what phone number they are coming from; there isn't a record of that information. Mr M has said he didn't make any of the calls. None are successful in releasing the payment.

Mr M has said he didn't listen to the answerphone message from Santander himself. His father heard it and passed on the three digit code to Mr M.

Mr M then received another spoof text message, similar to the earlier one, at 19:02. This time it said:

*Santander has noticed your debit card was recently used on 01-03-201719:02:02, at AMAZON ONLINE STORE for 9,182.17 GBP. If not you please urgently call fraud prevention on 03********* or Intl +443********* . Do not reply by SMS*

Mr M was prompted into calling Santander by this second spoof text. He thought his account was still under threat following what had happened earlier. He rang the number given in the spoof text, again connecting him to the fraudster but believing he was calling Santander. He didn't call the number given in the answerphone message as he hadn't listened to it himself; his father had passed on the code but not the phone number. He gave the three digit code to the person he spoke to as they said they needed the code to stop the transaction.

Santander then received a call, most likely from the fraudster, at 19:19 and the three digit code was given. This satisfied Santander that the online payment of £9,182.17, set up following the earlier amendment to the payee, was genuine and the money was released. The transfer left Mr M's account in an overdrawn position.

Here is a timeline of the key events:

16:32	Mr M receives a spoof text from the fraudster about an attempted payment to APPLE ONLINE STORE
16:56	The fraudster logs on to Mr M's online banking and amends a payee
16:57	Santander sends the OTP to Mr M's registered mobile
16:58	The OTP is entered successfully online and a payee is amended
17:05	The instruction to send a single transfer of £9,182.17 to the amended payee is made
17:06	Santander's security system calls Mr M's landline and leaves an automated message containing a three digit code
17:13	Attempts to verify the transfer with Santander's automated system begin
19:02	Final unsuccessful attempt to verify the transfer
19:02	Mr M receives a further text from the fraudster, again about an attempted payment to APPLE ONLINE STORE, this time for the amount of £9,182.17
19:19	Someone calls Santander and gives over the three digit code and the transfer is released

Mr M realised something wasn't right the next day when he logged into his online banking and saw the transfer out of his account. He contacted Santander to report the fraud and it began to investigate. It contacted the receiving bank and was able to recover £190.17, although it seems this wasn't actually refunded to Mr M at the time. But the rest of the money had already been removed from the account it had been sent to.

Mr M asked Santander to refund the rest of his money as he hadn't authorised the transfer out of his account and had been the victim of fraud. Santander considered the claim but said it wouldn't be refunding Mr M in full as he'd given away security information which made the transfer of funds possible. It did refund him £1,995.70 which represented the portion of the transfer made from Mr M's overdraft.

Santander said that had Mr M called the number left in the voicemail, as instructed, he would have discovered the transfer and been able to stop it.

Santander recognised there had been some problems with how it handled Mr M's fraud claim and so it paid him £80 for any distress and inconvenience suffered.

Mr M was unhappy with Santander's response. He believed he should have been refunded in full as he hadn't authorised the transfer. He thought it was particularly unfair given the spoof texts he received and which made the whole situation seem genuine. And in all the messages sent to him by Santander there was never any mention of a transfer being made out of his account meaning he had no idea that was happening. Santander didn't change its view and so Mr M asked us to investigate.

One of our adjudicators looked into Mr M's case and didn't uphold it. She said that although Mr M was convinced he was speaking to the bank he did give over security information. She thought it was more likely than not that he did give over the OTP as well as the code from

the voicemail. It was only because of his disclosure of those details that the transfer was made. And so she didn't recommend Santander refund Mr M.

Mr M asked for an ombudsman to review his case as he wasn't happy with the adjudicator's conclusions.

my provisional decision

On 21 December 2018 I issued a provisional decision on Mr M's complaint. After considering all the evidence and arguments presented by both sides, I was minded to conclude that:

- Mr M did not authorise the transactions in question;
- Mr M had not acted with gross negligence;
- Santander should fairly and reasonably refund the money obtained from Mr M by the fraudster, plus interest at the rate he would have received had the money remained in his account; and
- Santander should pay Mr M £300 for the trouble and upset he experienced.

Mr M responded to say he accepted the findings set out in my provisional decision.

Santander also responded to say it 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.

I've included the relevant considerations here for clarity, along with a summary of the findings from my provisional decision and my direction to Santander to put things 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 transfer from Mr M's account was made 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 (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 or 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 M 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 M's account

The following are extracts from the general Terms and Conditions applicable to Mr M's account at the time. These Terms and Conditions broadly reflect the provisions contained in the PSRs 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 provided its online banking terms and conditions, which state, *"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 M, unless Mr M with intent or gross negligence, failed to comply with the Terms and Conditions of the account and the obligations set out in Regulation 57.

Santander hasn't made it completely clear why it won't refund Mr M the full amount of money stolen from him. In its final response to him it discusses the disclosure of personal information and security details – including the OTP and three digit security code – by Mr M to the fraudster. It goes on to say that it was these disclosures that led to the money being transferred out of Mr M's account.

In these circumstances there are two key questions relevant to my consideration about what is fair and reasonable in the circumstances:

1. was the disputed transfer authorised by Mr M? *and*

2. if it wasn't, can Santander demonstrate that Mr M failed with intent or gross negligence either to comply with the terms and conditions of the account or to keep his personalised security details safe?

was the disputed transfer authorised by Mr M?

I'm not persuaded, on balance, that Mr M authorised the transfer of funds out of his account. I don't know exactly what was discussed between Mr M and the fraudster. But what does seem to be apparent – and largely accepted by all parties – is that Mr M gave the fraudster enough information for them to be able to access his online banking. And it also seems to be accepted that Mr M did so as he genuinely believed he was protecting his account from attack following the receipt of the spoof text messages.

Mr M has confirmed he gave over details such as his date of birth and customer number. He told us he isn't sure about what parts of his password he may have given though I think it's likely he gave over enough for the fraudster to gain access to his online banking. I've seen no evidence that would lead me to think the fraudster obtained those details from somewhere else.

We know the fraudster also used an OTP to amend an existing payee on Mr M's online banking. I'm satisfied that the OTP was sent to Mr M and indeed he's provided screenshots of his phone which show the message.

Mr M has said he's sure he didn't give the OTP to the fraudster. He thinks it must have somehow been automatically forwarded to the fraudster, and he's described how he felt he'd been coached through setting up call forwarding on his mobile.

I have considered the possibilities but there doesn't seem to be a reasonable explanation for how the text from Santander could have been received on another handset. Call forwarding, even if set up correctly on a handset, doesn't automatically forward on text messages. And I've not seen any evidence to suggest the steps described by Mr M would lead to text message forwarding. I'm not saying it could not have happened or even that it did not happen. Only that I think it's on balance more likely, based on the evidence I have, that Mr M did receive the OTP and read it out to the fraudster, at the fraudster's request. I can see why a fraudster would have wanted to coach Mr M through a call forwarding process as it could divert incoming security calls. But I believe that's unlikely to have meant text messages would also be forwarded.

I don't think there's been any duplication or swapping of Mr M's sim card here either. The bank's records indicate that there was some attempted contact on Mr M's mobile phone after the OTP was sent. And there's an entry recorded which suggests the sim was checked and came back as ok.

I've considered Mr M's recollections and, whilst I can't be completely certain, I'm more persuaded that he did likely give over the OTP. I think it's likely he did this in the belief that this was necessary to stop the payment he'd been told was leaving his account. He was clearly persuaded he was speaking with the bank and the fraudster had his confidence at this stage. And that lends itself to him being convinced into handing over the OTP.

But whilst I think it's more likely than not Mr M did pass on the OTP I don't think that means he authorised the transfer. There is no indication that he knew any payments would be leaving his account. On the contrary I think it's likely he thought what he was doing was to stop a payment. And it's the fraudster that has actually set up the payment online, not Mr M.

It's also the case that the transfer isn't actually made at the point the OTP is entered online. Santander flagged the transfer as suspicious after this point and they blocked it. That's when the call to Mr M's landline was made and the voicemail left.

Mr M has said he didn't pick up the message himself; it was relayed to him by his father. He then may not have been given the full content of the message. But even if he had there was no indication in the message that a transfer was being made out of his account. The message mentions being from Santander's fraud department. But there's no detail of any outgoing payment and nothing said about the purpose or reason for needing to call the bank.

This means that when Mr M called the fraudster again – believing it to be Santander – he still had no idea a payment was about to be made. He didn't know the code he was giving over would be used by the fraudster to release that payment.

The fraudster then used the code by calling Santander. It's only at this point there's any detail given about the transfer that's about to take place. But Mr M wouldn't have heard any of that information as he didn't make the call.

Mr M called the bank the following day having realised something was wrong. He was shocked to find a payment of over £9,000 has left his account. I don't think he had otherwise

been aware that was going to happen as the deception unfolded. It follows then that I'm satisfied that Mr M didn't consent to or authorise the transaction. He couldn't have done as he didn't know a transaction was about to take place.

My starting point then is that it wouldn't be fair and reasonable for Santander to hold Mr M liable for the transaction as I think, on balance, it was unauthorised. But I do need to go on to consider whether Mr M 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 M fail with gross negligence either to comply with the Terms and Conditions of the account, or to keep his personalised security details safe?

Mr M can't be said to have been grossly negligent solely on the basis that he gave away security information to a third party. I have to consider the circumstances in which that information was disclosed in order to reach a fair and reasonable outcome.

Mr M has been the victim of a sophisticated fraud. He was persuaded to give over personal information and online banking details. He was also likely tricked into giving an OTP before finally passing on a security code from an automated voicemail message. I don't believe, however, that on balance Mr M has been grossly negligent in falling for the tricks of the fraudster.

I've already set out how both the courts and the FCA have interpreted gross negligence and how it is a higher bar than ordinary negligence. And so I've gone on to consider Mr M's actions in the particular circumstances at hand and whether his actions fell so far below the standard of a reasonable person that it would be fair to say he'd failed with gross negligence to keep his security information safe or to comply with the terms and conditions of the account.

Gross negligence isn't an abstract concept and must be considered with regard to what was happening at the time. Mr M was the victim of a sophisticated scam involving what is termed 'smishing' as well as 'social engineering'. Both methods are used by fraudsters to lure people into a false sense of security and to believe they're talking to their bank. The illusion that's created is to make the victim act with urgency, the driving force behind that being the need to protect their account. I need to consider Mr M's actions with these factors in mind.

Mr M has provided us with copies of the text messages he received. It's clear they appear in the same chain of genuine texts he'd previously received from Santander. Mr M has said he was convinced it was from the bank and I've no reason to doubt him here. It's borne out by what happens after, with him contacting the number given in the text. It's a sophisticated method used by fraudsters to trick people into thinking they've received a genuine warning about suspicious activity on their account. And it creates the sense of urgency fraudsters rely on in getting people to act quickly. I can understand why the text wouldn't have raised suspicions for Mr M and I don't think it would have raised suspicions for many people, given the genuine and convincing appearance of the text.

I'm satisfied Mr M believed he was taking the right steps to protect his account when he followed the instructions given by the fraudster. That includes him calling the number in the text as well as being tricked into giving over personal and security details. I don't think he appreciated the risk at the time and so it can't be said he was indifferent to it or disregarded it. He genuinely thought he was stopping fraudulent activity on his account. And I think other reasonable people would have thought similarly.

Mr M has maintained that he didn't give over the OTP. I've already explained why I think it's more likely than not that he did. But that does leave me in a position where I don't have an explanation of the context in which it was handed it over. That is to say I don't know what was said by the fraudster to persuade Mr M into disclosing it. But I think it's most likely Mr M was persuaded to do so as the fraudster convinced him it was required to stop the payment referred to in the first spoof text message.

When it comes to the code provided in the voicemail Mr M has said the fraudster told him the code was required to stop the payment. And so it seems likely a similar explanation was given for the OTP. And I can see why, in the moment, Mr M thought he needed to act quickly to protect his account.

I wouldn't expect Mr M to know what steps might actually be necessary for stopping a payment. I also wouldn't really expect him to question what the steps might be either, given he believed that he was doing what was necessary. He had received what appeared to be genuine fraud alerts to his mobile followed by an actual voicemail alert to his landline. Mr M felt he had to act quickly to protect himself. He's described moving quickly from panic to feeling someone was helping him to protect his money. I think a reasonable person would have acted in a similar way to Mr M in the same circumstances.

Mr M was – not unreasonably – completely convinced by the fraudster that he was speaking to his bank and acting to keep his account safe. I don't think his actions fell so far below the standard expected of a reasonable person, in the same circumstances as to amount to gross negligence.

putting things right

As both parties agree, I now direct Santander to:

- refund Mr M's account with the total £9,182.17;
    - account should be taken of the £1,995.70 already refunded on 10 March 2017;
    - account should also be taken of the £190.17 recovered from the receiving bank but that was not credited at the time. It's unclear whether this money has been returned as yet;
- pay interest on the above amounts at the respective account interest rate, from the date of the withdrawal to the date of settlement. If Santander deducts tax from the interest element of this award, it should provide Mr M with the appropriate tax deduction certificate.
- pay compensation of £300 to Mr M. This has been a very worrying time for him, not receiving a refund for a transaction he didn't authorise, after having been the victim of the scam.

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

my final decision

I now direct Santander UK Plc to settle Mr M'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 M to accept or reject my decision before 1 March 2019.

Ben Murray
ombudsman