## complaint

Miss B is unhappy that Santander UK Plc won't refund payments from her 123 student account that she says she didn't authorise. Miss B says she was tricked by fraudsters into handing over information which they then used to transfer funds out of her account.

## background

Miss B held a 123 student current account with Santander. In March 2017 Miss B was the victim of a social engineering scam which involved 'vishing'. This is where a fraudster calls a consumer and uses a range of persuasive techniques to manipulate them into sharing personal information. Here the fraudster pretended to be from Miss B's bank, Santander, and convinced her to take certain steps and share information in order to gain access to her bank account and steal money from Miss B.

*what happened?*

Miss B says that, on 1 March 2017, she received a call from a fraudster pretending to be from Santander. She was told there was suspected fraudulent activity on her account from people claiming to be from HMRC. It's not in dispute that what happened was an act of fraud. So I have used the term "fraudster" throughout to refer to the third party involved.

Miss B thinks the fraudster knew she had been in contact with HMRC regarding a genuine tax rebate and that she may have fallen victim to a phishing email. As the day before she received the call from the fraudster she recalls divulging her card details on an email pertaining to be from HMRC. Miss B has said that, on realising it may be have been fraudulent, she has since deleted the email as she was concerned about viruses.

Miss B thought the call from the fraudster was plausible, as she had been dealing with HMRC and the fraudster knew a lot of personal information about her. She's told us she was led to believe she was being defrauded and that she had to act quickly.

Miss B was asked to provide three numbers from her five digit online security code, which she provided. She says the fraudster told her that she would receive a text message and that she'd need to read the code so that she could block the suspect payments from going out. Miss B received the text which said it was from Santander, which said use this code to pay the £800.

Miss B said she asked the fraudster why they wanted the code if it was to pay the £800 – she says she was told she had to give it to the fraudster to enable him to block the suspicious payments.

Miss B said she received another text with a different code – but she only recalls giving one code out to the caller. She's said she became suspicious when the caller asked her to give him the two remaining numbers from her security code – at this point she told the caller that she was going to call Santander.

These codes were One Time Passcodes (OTPs) from Santander. Miss B has said that she deleted the texts. Santander has told us the text messages actually read:

*'OTP (code) is to SETUP A NEW PAYEE on account ending XXXX. Never share this code with anybody. Please call us immediately if you did not request this' and*;

*'OTP (code) is to make a new payment for (Amount) to account ending XXXX. Never share this code with anyone. Call immediately if you did not request this'*

Miss B gave the code to the fraudster and, shortly afterwards, £800 was transferred out of her account to a 'new' payee that the fraudster had set up.

Miss B ended the call with the fraudster and called the genuine Santander number. Santander confirmed to Miss B that it wasn't them she'd been speaking to and that it had been trying to contact her while she had been on the phone.

Miss B already had online banking set up on her account and the fraudsters got access to this. Information from Santander about the activity on Miss B's online account shows that the "'forgotten customer ID option" was selected. Santander has said this can be requested if forgotten, just by providing personal information. Santander said the partial details of the security number that Miss B gave the fraudster enabled them to then activate her online banking.

Santander has said that three OTPs were generated and a text message was sent for each one, all three were validated – it's said that three new payees were set up and a payment of £800 was made to each of these new payees. The first transaction for £800 was processed, but Santander has said it was successful in preventing the other two transactions for £800 going through.

Santander has said it attempted to recover the 'successful' transaction shortly after speaking to Miss B. But on contacting the beneficiary bank (Barclays) it wasn't possible for it to be recovered. So overall, Miss B suffered a loss of £800 from her Santander account.

Santander says as there were three payments set up it triggered its Fraud Detection system and Miss B would have received an automated call. Miss B has said that she received a voice message from Santander saying she was potentially being defrauded, which she picked up after she'd finished the call with the fraudster. Miss B said this genuine voice message and the genuine fraud call from Santander were very similar to the fraud call, which she says indicates what an easy mistake this was to make.

Santander has said that its Fraud Detection System put a block on Miss B's account which caused the second and third transactions to 'pend'. When Miss B contacted Santander and confirmed the transactions to be fraudulent, the agent she spoke to was able to cancel them. Below are some of the key timings of the online banking activities during the scam, according to Santander's online banking records:

| **date** | **time** | **online activity** | **amount** | **transaction outcome** |
|---|---|---|---|---|
| 1/3/2017 | 10:25:17 | Fraudsters accessed Miss B's online banking via the "forgotten password" route | | |
| 1/3/2017 | 10:28;10 | OTP sent via SMS | | |
| 1/3/2017 | 10:28:43 | first new payee set up | | |
| 1/3/2017 | 10:28:43 | OTP validated | | |

| | | | | |
|---|---|---|---|---|
| 1/3/2017 | 10:28:47 | payment made to first new payee | £800.00 | successful |
| 1/3/2017 | 10:31:38 | second OTP sent | | |
| 1/3/2017 | 10:32:12 | second OTP validated | | |
| 1/3/2017 | 10:32:12 | second new payee set up | | |
| 1/3/2017 | 10:32:15 | payment made to second new payee | £800.00 | blocked |
| 1/3/2017 | 10:32:47 | third OTP sent | | |
| 1/3/2017 | 10:33:12 | third new payee set up | | |
| 1/3/2017 | 10:33:12 | third OTP validated | | |
| 1/3/2017 | 10:33:14 | payment made to third new payee | £800.00 | blocked |

Miss B reported the scam at 10:48 on 1 March 2017. This was around 15 minutes after the final transaction was attempted and around 20 minutes after the first transaction had been sent.

The beneficiary bank has said the money for the first transaction of £800 left the receiving account at 10:39, which was around 10 minutes after it had been sent by Santander.

Miss B acknowledged that she'd played a part in the fraud through divulging certain information. But she's said this is the first time that such a highly plausible fraud has been attempted on her and she was panicked into doing what she thought was the right thing to do.

Miss B has also questioned why the transaction wasn't stopped immediately when Santander suspected it to be fraudulent. She's said even if this wasn't possible it should have been possible for the receiving bank to have blocked it. In summary she concludes the money could have been retrieved if action had been taken quickly enough.

Santander didn't refund Miss B. It was sorry Miss B had been the victim of a scam but it said it hadn't upheld Miss B's complaint on the basis that she'd divulged sufficient information for the scammer to gain access to her online banking, set up 3 bill payments and make transfers from the account. It says the fraudster was only able to gain access to the funds because of their manipulation.

Santander said it has system security in place which was bypassed through manipulation. It added that it had exhausted all avenues in pursuing the funds.

It says it sent important security messages to Miss B via her internet banking facility in November 2016 and January 2017. It says the emails provided information on how customers are being scammed and how to keep details secure by not divulging information such as OTPs. Overall Santander didn't think it could be held liable for Miss B's loss.

As Miss B wasn't happy with Santander's final response she brought her complaint to our service and it's been passed to me for a decision.

**my provisional decision**

On 28 January 2019 I issued a provisional decision on Miss B's complaint. After considering all the evidence and arguments presented by both sides, I was minded to conclude that:

- Miss B did not authorise the transactions in question;
- Miss B had not acted with gross negligence;
- Santander should fairly and reasonably refund the money obtained from Miss B by the fraudster, plus interest at the rate she would have received had the money remained in Miss B's account; and
- Santander should pay Miss B £200 for the trouble and upset she experienced.

Miss B responded to say she 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 an extract of the findings from my provisional decision, as well as 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 transfer from Miss B'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 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 Miss B did fell so far below the standard expected of a reasonable person that it would be fair to say she failed with gross negligence to keep her personalised security details safe or to comply with the Terms and Conditions of the account.*

***the Terms & Conditions of Miss B's account***

*Santander has referred to its Terms and Conditions when considering Miss B's actions.*

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

*7. "7.1 Notification of Unauthorised or Incorrect Payments If you believe that a payment on your account was not authorised by you or was made incorrectly, you must notify us as soon as possible either at a branch or by telephoning us….*

*"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….. 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…*

*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:…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 Santander 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."*

*13.1 "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…"*

***key questions***

*In my view the above relevant considerations mean that, if the transactions were unauthorised, it would be fair and reasonable for Santander to refund the amount stolen from Miss B, unless Miss 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 its final response to Miss B, Santander doesn't give a clear reason for deciding not to refund the amount stolen. It simply says that the claim was reviewed by a member of its investigation team and Miss B was advised the claim had been declined. It goes on to say that it can't be held responsible for the loss on Miss B's account.*

*Santander has told us the reason for deciding not to refund the amount stolen from Miss B is that the funds wouldn't have been sent if Miss B had refused to provide the OTP. It's said that the compromise of personal data was made at the customer's end. So it doesn't think it's at fault for the loss, as under the Terms and Conditions of the account it's not liable for a loss incurred when personal security details are disclosed.*

*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 Miss B? and;*

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

***were the disputed transactions authorised by Miss B?***

*On the balance of evidence I'm not persuaded that Miss B authorised these transactions from her account. I'll explain why.*

*Miss B has told us that the fraudster knew a lot of personal information about her. Miss B thinks this might have been through a 'phishing' email she had received pertaining to be from HMRC, whom she had genuinely been in contact with about a tax rebate. While it's not completely clear how the fraudster had obtained personal information about Miss B, what Miss B has described is very possible.*

*I've not seen anything that enables me to say for sure how the information was obtained. Fraudsters use highly complex and varied methods to gather information from what can be many different sources.*

*Information received from Santander about the activity on Miss B's online account shows that the "forgotten customer ID option" was selected. When this happens a customer can get a reminder of their customer ID by providing personal information, such as full name, date of birth and card/account number.*

*I don't know exactly what was discussed between Miss B and the fraudster, but it appears as though, along with personal information the fraudster already had about Miss B, she gave the fraudster enough information for them to gain access to her online banking. The information Miss B divulged was all in the context of protecting her account and trying to stop unrecognised transactions, rather than to authorise payments.*

*Miss B accepts she gave over one OTP to the fraudster, but she's done so on the understanding that this was to allow unrecognised payments to be stopped. Given what happened next, it's clear the fraudster used this OTP to set up a new payee. The fraudster then transferred money out of Miss B's account to payees unknown to her.*

*Miss B recalls that she did receive a second text, but that she didn't give this over as she became suspicious. The activity records that Santander has provided suggest that three OTPs were sent to Miss B and each were validated. On balance, I think it most likely that there were three OTPs sent to Miss B's phone and that she most likely gave all of these over to the fraudster. I say that as without these the fraudster would've been unable to progress with setting up the new payees.*

*Miss B describes the situation surrounding the call with the fraudster, and the level of trust built through what seems to have been the considerable sophistication of the scam. I think in those circumstances it would have been understandable that Miss B, believing she was speaking with her bank, gave over the codes in messages she'd been sent – even though she may not have recollected it after the event.*

*I've not seen any compelling evidence that suggests to me that, at any point during the call with the fraudster, Miss B knew that any payments were going to be made from her account. Miss B says she thought she was speaking to somebody from Santander, they told her the text would be coming and she gave it to them as she thought it was to stop an authorised payment. For the reasons explained, I think it's most likely this is also what happened with the second and third OTPs, even though Miss B may not have recalled giving this information over.*

*Regardless, it's clear the fraudster used the OTP codes to set up three new payees on the account. The fraudster then transferred money out of Miss B's bank account to new payees unknown to her.*

*Miss B recalls becoming suspicious during the call with the fraudster and chose to end the call. While on the call with the fraudster she'd received a message from Santander's fraud department and so she called the bank to raise her suspicions. During this call Miss B told Santander that she didn't recognise the disputed transactions.*

*Santander's fraud prevention system had been triggered, seemingly due to the unusual activity on Miss B's account of three new payees being set up. This resulted in the second and third payments for £800 pending – once Miss B confirmed to Santander these were not authorised by her, it was able to cancel these. From the information I've seen Santander did act promptly in contacting the beneficiary bank about the first payment for £800 – it was unfortunate that it wasn't able to recover the funds due to the money being moved on quickly on from the beneficiary bank.*

*Miss B has said that it should have been possible for the beneficiary bank to block the payments. But I haven't considered a complaint against the beneficiary bank in this decision.*

*Overall, I don't think Miss B was aware that any payments were being made from her account. On balance, I'm persuaded she didn't consent to or authorise these transactions to be made from her account.*

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

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

*It is not enough to say Miss B was grossly negligent simply because she shared security details for the account. Careful consideration needs to be given to the circumstances under which those details were shared.*

*Miss B was tricked by a fraudster into giving some account security information. Miss B was also then tricked into handing over OTP codes which allowed new payees to be set up. However, on the balance of evidence, I don't think it would be fair or reasonable to say that, in falling for these tricks and failing to keep her security details safe, Miss B was grossly negligent and I'll explain why.*

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

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

*Gross negligence isn't an abstract concept. It's important to take into account all the circumstances when considering whether an individual's actions amount to gross negligence. The scam here involved "vishing", "social engineering" and most likely "phishing", where the fraudsters use a range of sophisticated techniques to trick, deceive and manipulate their victims into giving out confidential information. Here Miss B was made to believe she was talking to her own bank, needing to act quickly to protect her bank account which she was told was being used for fraudulent spending. So I've thought about Miss B's actions in that context, and considered her overall actions.*

*Miss B thought the text message she was sent was to stop a payment, as this is what she was told by the caller, who she thought was from her bank. This is a sophisticated method used by fraudsters to trick their victims into a sense of security and safe environment 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 obvious suspicion from Miss B – or any reasonable person in these circumstances.*

*I do not think, at the time, Miss B thought anything other than the actions she was taking were for any other purpose than to prevent a fraudulent payment leaving her account and to secure her bank account. Rather than appreciating the risk she was taking by following the fraudster's instructions but disregarding or being indifferent to them, she was under the opposite impression that if she didn't follow those instructions she was at risk of losing money.*

*Miss B recalls receiving three OTPs, but only divulging one to the fraudster. Although, for reasons already explained I think it likely all three codes were received and given to the fraudster. In this case, it seems likely that the fraudsters convinced her that the codes were*

*needed in the process of protecting her money and the various stages the bank needed to go through to do that. And I wouldn't expect Miss B to know what Santander's processes are for stopping a payment or to necessarily question what she was being asked to do — because she genuinely believed she was working with her bank to protect her account. She reasonably felt worried about the security of her bank account, and felt a corresponding pressure to act. In similar circumstances, I think a reasonable person would've acted in the same way that Miss B did here.*

*So on balance I don't think the codes provided by Miss B to the fraudster were enough to break the spell she was under. I've also considered that Miss B acted promptly in contacting Santander to raise her concerns when they dawned on her. This is what she was expected to do under the Terms and Condition of her account. Overall, I'm not persuaded that her actions fell so far below what a reasonable person would do in the circumstances to amount to gross negligence.*

***warnings***

*Santander refers to a number of things it has done to raise the general awareness of fraud risk amongst its customers, including specific warnings which it says Miss B would have had which provided information on how customers are being scammed and how to keep details secure.*

*But even if Miss B engaged with these things it doesn't follow that she was grossly negligent for falling victim to fraud thereafter. Nor would it be necessarily be fair to say Miss B was grossly negligent if she did not engage with these things and then fell victim to fraud. I am required to consider whether what Miss B did, or failed to do, fell so far below the standard of a reasonable person that it would be fair to say she failed with gross negligence to keep her personalised security details safe or to comply with the terms and conditions of her account.*

*To be clear, 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 messages 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 Miss B's failure to read or heed 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 Miss B's account with £800; 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 Miss B with the appropriate tax deduction certificate.

- I think it would be fair for Santander to pay Miss B a further £200 compensation. This is to recognise that Miss B has been without her money for some time and for the trouble and upset I've no doubt this would have caused.

Under PSR 2009, and the Terms and Conditions of the account which reflect that legislation, Santander is entitled to hold Miss B responsible for the first £50 of their loss. If it intends to do this, it can take this amount from the £800, before adding the interest element.

**my final decision**

As I've concluded above I now direct Santander UK plc to settle Miss 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 Miss B to accept or reject my decision before 23 April 2019.

Stephen Wise
**ombudsman**