DRN-4453241

The complaint

Miss Z complained because Santander UK plc refused to refund her for transactions she said she didn't make.

What happened

On 1 July 2023, Miss Z received a text from Santander saying that her account had gone into an unauthorised overdraft. Miss Z logged onto her online banking, and saw there were four payments to an online retailer, for £98, £465, £480 and £425, totalling £1,468. Miss Z rang Santander and said she hadn't made the payments, and she also went to a branch.

On 5 July, Miss Z spoke to Santander again, and was told the payments had been authorised through her phone. Miss Z said she hadn't received any codes. She pointed out that as her account was in unauthorised overdraft, she had to borrow money to put money into her account.

Santander didn't uphold Miss Z's claim for a refund. It initially said that the payments had been authenticated using a one-time passcode sent to Miss Z's phone. But this was incorrect, and they'd actually been authenticated within Miss Z's app. In Santander's final response to her complaint, it said that the payments had been authenticated using another level of authentication through her mobile banking. It said this would have required Miss Z's login information, which was why it had discussed with her whether this could have been compromised. But Miss Z had said there was no possibility of that, and she hadn't been contacted or instructed to make the payments. So Santander refused to refund Miss Z.

Miss Z wasn't satisfied and contacted this service. She said no-one had access to her phone or card details, and no-one had access to her phone or card, and she wouldn't ever share these with anyone. She said that her physical and mental health had suffered, and Santander was supposed to protect money not allow fraudsters to steal it. She said someone had hacked her account and stolen her money. She wanted Santander to refund her; to pay the charges she'd incurred through late direct debits; and compensation for the way she was treated by Santander's fraud team, and the stress and emotional distress.

Our investigator didn't uphold Miss Z's complaint. He said that Miss Z had said she had her mobile and card at the time of the transactions, and had also said she hadn't allowed anyone else to have access to these. The payments had been made in app. And although Miss Z had said she didn't have biometric Face ID on her phone, Santander's computer logs showed that on 13 April, Miss Z had registered her phone for online banking and the same day had enabled biometrics.

Miss Z didn't agree. She said her original questions hadn't been answered, and as the victim she had the right to ask them. She wanted proof of the address the goods had been sent to; proof of signature and email used; proof that her full correct name had been used; and proof of a one-time passcode sent. She was also unhappy because the transactions had been ''pending'' when she'd originally phoned, and Santander hadn't stopped them. She said she'd asked for this many times. She said Santander had changed what it was saying, having originally said there had been a one-time passcode sent and then saying it had been

approved in app. Miss Z said this was because Santander didn't want to be held accountable and pay her back the money.

Miss Z asked for an ombudsman's decision.

What I've decided – and why

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

There are regulations which govern disputed transactions. The relevant regulations here are the Payment Services Regulations 2017. In general terms, the bank is liable if the customer didn't authorise the payments, and the customer is liable if they did authorise them. So what I need to decide is whether Miss Z, or someone else without her authority, is more likely than not to have authorised the four disputed payments.

First, I'd explain two preliminary points. ''Pending'' transactions can't be recalled by the sending bank, so Santander couldn't have stopped the transactions when Miss Z first contacted it. Also, the technical evidence here doesn't show all the information which Miss Z has requested. What the computer evidence shows is things like the date and time; amounts; merchant name; technical details about how the payment was made; and the IP address (a unique computer identifier). In other words, it's about the payments, and not about the purchase information. So the Santander computer information doesn't show, for instance, the information which the person making the payment would have supplied to the merchant - what was purchased, where the goods were sent, and the full name of the person buying them. Miss Z has also asked for proof of signature and email used to place the order, but the disputed transactions were made online so no signature would have been involved, and not necessarily any email address. The key thing that determines the outcome here is the technical computer evidence about how the transactions were carried out. That provides information from which I decide what's more likely than not to have happened.

I've considered the computer evidence in detail very carefully, and I asked Santander for more technical information on several occasions.

I agree with Miss Z that Santander was incorrect when it initially told her that the four disputed transactions had been authenticated using a one-time passcode sent to her phone. This isn't what the coding on the computer logs show. A subsequent Santander employee picked this up, and pointed out on the notes that in fact the coding meant the disputed transactions had been authenticated in app. So Santander made an error about this, but this doesn't in itself alter the outcome. What the coding does show is authentication in app, so this is what I've focused on.

Miss Z said that she still had her phone, and that she hadn't allowed anyone to have access to it. This is a key issue here, because the computer data shows that the transactions were carried out on her mobile phone. It also shows that Miss Z registered that phone on her account on 13 April. The phone number registered that day is the same which Miss Z supplied to us as her contact number for her case, so I accept that the phone registered that day was Miss Z's phone, and not a third party who might have registered their own phone.

I've considered the debate about biometric data. Miss Z says that she didn't have biometric security on her phone. Santander's records show that biometric data was ''enabled'' on Miss Z's phone on 13 April. But the computer logs of the actual transaction don't show whether biometric data was or wasn't used for these transactions. Being ''enabled'' doesn't prove that biometrics were used for these particular transactions, only that biometrics could be used on the phone.

The computer logs show that the transactions were authenticated using the app – but they don't show how the app was accessed. I find that it isn't relevant here whether the app which was used was accessed by biometric security, or by passcode/PIN. One of these methods must have been used to pass security to access the app. It doesn't make any difference to the outcome here, whether it was biometric or passcode/PIN. What matters is whether any third party could have accessed whichever was used. It's not likely any third party could have compromised a biometric, but it's also unlikely that any third party could have accessed her passcode / PIN when Miss Z said she hadn't let anyone else know this. So, whichever method was used, it's not likely a third party could have obtained what they needed to pass the security.

Miss Z still had her phone, on which the transactions were made. And she hadn't let anyone else know her security information to access the app. She hasn't said that anyone at work or leisure could have obtained her details; nor that she'd been scammed into making the payments by a third party.

The transactions were carried out in the middle of the night. And they were made from an IP address which – contrary to what Santander said – Miss Z hadn't used before. They were made within a very short space of time, and emptied Miss Z's balance. All of this can sometimes be indicative of fraudulent transactions.

But the sticking point here is that the transactions were carried out on Miss Z's phone which she said she still had, and using either biometrics or a passcode/PIN which she says no-one could have known. In view of that, I can't see how any third party fraudster could have carried out the transactions, and it has to be more likely than not that either Miss Z, or someone known to her who'd had access to her phone and security information, carried them out. So I don't uphold this complaint.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss Z to accept or reject my decision before 8 February 2024.

Belinda Knight
Ombudsman