

The complaint

Mr B complained because Santander UK Plc refused to refund him for a transaction he said he didn't make.

What happened

On 5 July 2023, an internet payment for £132 debited Mr B's Santander account. The payment was made using a mobile payment service. There were also several other payments to a different organisation which were authorised in the same way, but those were never claimed by the merchant and didn't debit Mr B's account.

Mr B contacted Santander to report the transactions as fraud. On 7 July, Santander rejected Mr B's claim. It said that it couldn't refund him, because the IP address (a unique computer identifier) used to make the disputed payment had been used by Mr B before, for genuine banking activity.

Mr B didn't agree, and complained. Santander reviewed his complaint, but still didn't uphold it. In Santander's final response letter, it explained that:

"When a customer adds their card to a device, a unique 16 digit Device Primary Account Number (DPAN) is assigned, which connects the device an the card. We can evidence that the DPAN used to process the disputed transaction for £132 to [name of recipient organisation] has also been used for genuine undisputed activity.

On review, we also confirm that the IP address used to complete the [name of mobile payment service] registration has also been used for genuine undisputed activity."

Mr B wasn't satisfied and contacted this service. He said his phone was secured by Touch ID and a passcode, and no-one else had access to his phone. He also said he hadn't ever let anyone else use his card. He said he kept his card in a safe place and used the mobile payment service.

Our investigator didn't uphold Mr B's complaint. She said Santander had provided evidence that the disputed transaction on 5 July had been made using the mobile payment service which had been set up on 17 May. Whoever had set this up must have had Mr B's full card details as well as access to his phone. And in view of what Mr B had said about how his phone was secured, with no-one else having access, the investigator couldn't see how any unknown third party could have made the transaction.

Mr B didn't agree. He said surely there were cameras at the place the money had been taken. The investigator explained that the payment had been an internet payment., and also said that transactions to the global technology company named as the recipient on the bank statement didn't always show as the name of the actual company paid. Mr B said he hadn't given access to his phone or details, but someone might have been able to get access without his knowing. Mr B said there must be a way of finding out where the recipient organisation was and what it sells. He 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 I've considered whether it's more likely than not that Mr B carried out the disputed transaction himself. I've only considered the £132 disputed transaction, because the other transactions which were also authorised on 5 July never debited Mr B's account.

The technical evidence is useful here. It shows that the mobile payment service used to make the disputed transaction was set up on Mr B's account on 17 May. Setting up this service was done by sending a one-time passcode (OTP) to Mr B's registered phone, which was then authorised. Mr B's evidence is that his phone was secured by biometric security (Touch ID) and a passcode, and that no-one else had access to his phone.

In his reply to the investigator, Mr B said that someone might have been able to get access to his phone and security without his knowledge. But he hasn't offered any possible way in which this might have happened. In view of Mr B's evidence about biometric security, and a passcode, to protect his phone, I can't see how any third party could have set up the mobile payment service on Mr B's account.

And even if a third party fraudster had somehow managed to set up the mobile payment service on Mr B's phone on 17 May, it's most unlikely they'd have waited until 5 July before making a transaction. Fraudsters tend to maximise their gain as quickly as possible. I also note that at the time of the disputed transaction, Mr B had several thousand pounds in his account. It's most unlikely any fraudster with access to Mr B's account would only have taken a transaction for £132 when there was a much higher balance available.

Other technical evidence shows the IP address from which the online £132 disputed transaction was made on 5 July. It's an address which Mr B had used before, for payments he hasn't disputed. And as Santander explained in its final response letter to Mr B, the DPAN used to process the disputed transaction was also used for activity which Mr B hadn't disputed.

So I find that it's more likely than not that Mr B carried out the disputed £132 transaction himself.

It's possible that Mr B simply doesn't recognise the transaction, because the name of the recipient on the statement is a global technology company which provides services to multiple organisations. But given the full discussion with Santander about this transaction, I'd have expected Mr B to have remembered it reasonably quickly after first disputing it. I note that after the investigator's view, Mr B said there must be a way of finding out where the recipient organisation was and what it sells. Mr B could contact the organisation himself if he wishes to. But it isn't Santander's responsibility to do that. As I've set out above, what matters here are the Payment Services Regulations, and whether it's most likely that Mr B carried out the transaction himself. I've found that it's more likely than not that Mr B did so, so I don't require Santander to refund him.

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 Mr B to accept or reject my decision before 14 March 2024.

Belinda Knight
Ombudsman