DRN-5302058

The complaint

Mr A complained because Santander UK Plc refused to refund him for two payments which he said he didn't authorise.

What happened

On 16 October 2024, Mr A contacted Santander. He said he hadn't authorised two payments which had been debited to his credit card. One was for £1,450 on 13 October, and the other was for £2,099 on 14 October. The transactions had been carried out using Apple Pay.

Santander refused to refund Mr A. It told him that it had sent him a One-Time-Passcode (OTP) on 13 September. This had been sent to Mr A's registered mobile number. The OTP had then been correctly entered in order to authorise Mr A's card being used via Apple Pay. A month later, Apple Pay was used to make the two disputed transactions.

Mr A told Santander that the text message sending him the OTP wasn't on his phone. But Santander didn't agree to refund him, and Mr A complained.

In Santander's final response letter, it said that Apple Pay had been set up using a OTP which had been sent to Mr A's registered phone number, and which had then been correctly entered. Santander said that the two disputed payments hadn't needed any extra authentication because the initial setup of Apple Pay had been verified by the OTP on Mr A's registered phone number.

In response to Mr A's comment that there wasn't a text with a OTP on his phone, Santander suggested he should contact his network provider to discuss any potential redirections on his account. Santander also discussed any potential scam calls, texts or emails, but Mr A didn't recall any, and knew he shouldn't provide anyone else with a OTP. He said he also hadn't downloaded any apps that allow a third party to view his phone.

Santander couldn't see how the OTP had been compromised, so it didn't uphold Mr A's complaint as fraud.

Mr A wasn't satisfied, and contacted this service.

He said he wanted a refund from Santander for the total of the two disputed payments, which came to £3,549. He also said he'd been distressed and had lost confidence in the banking system.

Mr A told our investigator that on 13 September, his SIM card had stopped working. The next day, he went to a phone shop, where his SIM card was replaced in front of him. He said his phone had remained with him the whole time, and never left his sight. He also said that he hadn't used his Santander credit card in over two years. He was still in possession of his credit card, but after the incident he'd been sent a replacement card.

Mr A added that there had recently been further attempts to make payments on his credit card in November and December 2024, but these hadn't debited his account.

Our investigator didn't uphold Mr A's complaint. She said that the token to process the payments had been set up using a OTP, which had been sent by text to Mr A's phone. He'd said no-one else had access to his phone, and he hadn't shared his credit card details. So it wasn't possible that anyone else could have accessed his text messages or set up the Apple Pay token. The investigator wasn't persuaded that Mr A's account of his SIM being replaced on 14 September was a viable compromise of the OTP. Nor did it shows how a third party could have obtained the details to set up the Apple Pay token. So she found that Mr A was liable for the payments.

Mr A didn't agree.

He spoke to the investigator about the visit he said he'd made to a phone shop around 4pm on 14 September. But the investigator pointed out that it appeared that the token had been set up around 7pm that day - after the SIM problem had been resolved at the phone shop. And Mr A had said the shop assistant hadn't taken the phone from Mr A's sight.

Mr A then said that he'd been receiving fake letters and emails. He sent a copy of one, relating to an invoice which was dated 14 October. And he also said that he'd just found that he'd had a text from Santander at 8.50am on 13 October which said ''*You registered a new device for Apple Pay on 13 September 2024 but haven't used it yet. If this wasn't you with your device, please call us to have the device removed.''*

Mr A said that he'd been a victim of fraud, and criminals had stolen money from his credit card without his permission. 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.

What the Regulations say

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.

The regulations also say that account holders can still be liable for unauthorised payments under certain circumstances – for example if they've failed to keep their details secure to such an extent that it can be termed ''*gross negligence.''*

This means that what I need to decide is whether it's most likely that Mr A, or a third party fraudster, carried out the disputed transactions.

Who is most likely to have carried out the disputed transactions?

I've seen the computer evidence which shows that the OTP was sent to Mr A's registered phone number. That phone number was also used for other genuine purposes, and it's the number which Mr A provided to this service when he contacted us. So I'm not persuaded that this OTP didn't reach Mr A. It's most likely that it was Mr A who entered the correct OTP, which authorised his Santander credit card being used via Apple Pay.

I can't see how anyone else could have obtained Mr A's card details and the OTP from his phone. He said no-one else had access to his phone and he never shared his credit card details with anyone. I'm not persuaded by Mr A's suggestion that his trip to a phone shop on

14 September proves that someone else authorised the transactions. As the investigator pointed out, the timing is wrong. Also, Mr A had said the phone remained in his sight throughout the SIM change.

I also consider that if a third party fraudster had had access to Mr A's account via Apple Pay in mid September, they wouldn't be likely to have waited a month before spending on it. Fraudsters normally maximise their gains as quickly as possible.

Mr A also told the investigator, after she issued her view, that he'd found a text message from Santander on 13 October which said that Apple Pay had been registered on 13 September but ''*if this wasn't you with your device please call us.''* It was immediately after this October text that the disputed transactions happened. But it wasn't until 16 October that Mr A rang Santander. And what he said then was that he'd seen payments which he said he hadn't authorised. He didn't mention the text of 13 October. If Mr A hadn't set up Apple Pay himself, I'd have expected him to have phoned Santander about it immediately on 13 October.

I've also taken into account the fact that Mr A's evidence has varied during the course of this complaint:

- Mr A told Santander that he hadn't received any potential scam calls, texts or emails and he assured Santander that he hadn't downloaded any apps that would allow a third party to view his phone. But after our investigator issued her view, Mr A claimed he had indeed been receiving fake letters and emails.

- Mr A told Santander he didn't recall having any service issues with his phone. But he told our investigator that his SIM had stopped working on 13 September and he'd gone to a phone shop where the SIM was changed.

The change of evidence makes Mr A's account of events less credible.

Taking all these factors into account, I consider it's more likely than not that Mr A authorised the disputed transactions himself. So Santander doesn't have 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 A to accept or reject my decision before 5 June 2025.

Belinda Knight
Ombudsman