

The complaint

Mrs P complained because Santander UK Plc refused to refund her for transactions which she said she didn't authorise.

What happened

Mrs P disputed several payments which had debited her account in February 2024.

This decision is about two payments totalling £1,027.90: one for £877.90 and one for £150 which had taken place on 23 February. Initially Mrs P also disputed a payment for £84.97 on 21 February, but later recognised this payment and said she'd received the goods. Mrs P also disputed later payments, after she said she'd been scammed. That dispute about the later payments has been dealt with separately, and this decision only covers the two payments on 23 February totalling £1,027.90. These two payments were made by debit card online.

Mrs P told Santander that she still had her phone, and she hadn't made either of the two payments. Santander refused to refund Mrs P, and Mrs P complained.

In Santander's final response to Mrs P's complaint, it said that the reason it had refused her claim was that both payments had been made using her genuine device. They'd been verified using in-app authorisation, and used a One Time Passcode (OTP) which had been sent to Mrs P's registered mobile.

Mrs P wasn't satisfied and contacted this service. She said that she had only received a OTP for the £150 payment, not the £877.90 payment. She said she'd only received the OTP for the £150 payment a long time after the payments had been made. In reply to the investigator's questions, Mrs P said her phone and her Santander app were protected by Face ID, and no-one else had access to her phone. She hadn't lost her phone and still had it.

Our investigator didn't uphold Mrs P's complaint. She explained that she'd seen that a OTP had been sent to Mrs P's registered number. Mrs P had said she didn't receive this until around 12 hours after the transaction had gone through – but the investigator pointed out that the transaction couldn't have gone through without this OTP to authenticate it. The investigator said that it was most likely that Mrs P had authorised the transactions or had allowed someone else to make them.

Mrs P didn't agree. She said she hadn't received a OTP, text or phone call for the £877.90 payment, and she hadn't received a OTP for the £150 payment until after the payment had gone through. She said she'd taken her later complaint about a scam and other transactions to the police who were investigating.

Mrs P 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 this decision does and doesn't cover

I'm aware that Mrs P said scammers phoned her at 11.35am on 23 February 2024, and she said that they then gained access to her account as a result of that call

The two disputed transactions which I'm considering took place at 00:32am and 00:36am on 23 February. I can't see that any scam call around 12 hours later could have led to or enabled the two disputed transactions I'm considering here.

Mrs P's complaint about later transactions, after the call she said she'd had from scammers, has been dealt with separately.

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*."

So I've considered who is most likely to have authorised the two disputed payments totalling £1,027.90.

Who is most likely to have authorised the two disputed payments?

I've looked at the technical computer evidence about the payments. This shows that the device used to make the payments was the one registered to Mrs P's account. She still had that phone device, and both her phone and access to her Santander app were protected by Mrs P's biometric Face ID. So it's hard to see how any third party fraudster unknown to her could have carried out the payments.

The card information provided to make both secure e-commerce transactions matched Mrs P's card details. This included the unique 3-digit security number, the CVV code.

I've also looked at the audit trail information about the OTP, which shows it was sent to Mrs P's registered number. Mrs P said she didn't receive this on her phone until some 12 hours after the payments had gone through. But the records show that the method of authentication for the payment was the OTP. So the payment couldn't have gone through without this being correctly entered. Mrs P said no-one else had access to her phone.

So I can only conclude that Mrs P herself, or someone she allowed to make the payments, carried out the disputed transactions. If she allowed someone else to have access to her phone and app (including opening it for them using her biometric Face ID), it counts as Mrs P authorising the transactions. So Santander doesn't have to refund her.

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 Mrs P to accept or reject my decision before 7 July 2025.

Belinda Knight
Ombudsman