DRN-5912853

The complaint

Mrs F complains Santander UK PLC ("Santander") refuses to refund her for transactions on her account she says she didn't authorise.

What happened

The facts of this complaint are well known to both parties, so I won't repeat them in detail here.

In short, Mrs F says she checked her online banking on 29 November 2024 and noticed a significant sum of money missing from her balance. So, she contacted Santander to complaint about fraud on her account. Mrs F says the transactions on her account between 8 October 2024 and 28 November 2024, made with card ending *2765, were all unauthorised. She says she didn't receive a new card after hers expired in September 2024, and she didn't update the bank of her new address. So, she thinks someone else gained possession of her new card and made these unauthorised transactions. She would like Santander to refund all the transactions in dispute as unauthorised.

Santander didn't uphold Mrs F's complaint on the basis that the evidence shows most of the transactions were authorised via "in app" notifications on her registered device from her usual IP address. It also said that some transactions were verified via a one-time passcode (OTP) sent to her registered phone number. And as Mrs F says she had possession of her device, it must have been her who authorised these. So, no money was refunded.

Mrs F brought her complaint to our Service and our investigator considered everything that had been provided. Overall, he didn't think it would be fair to ask Santander to refund the payments made as the evidence suggested they were authorised. Mrs F was unhappy with this outcome, so the complaint has been passed to me for a final 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.

When considering what's fair and reasonable, I'm required to take into account relevant law and regulations; the regulator's rules, guidance and standards; the codes of practice; and, where relevant, what I consider good industry practice at the relevant time.

Where there's a dispute about what happened, and the evidence is incomplete or contradictory, I must make my decision on the balance of probabilities – in other words, what I consider most likely to have happened in light of the available evidence.

Generally speaking, Santander is required to refund any unauthorised payments made from Mrs F's account. Those rules are set out in the Payment Service Regulations 2017. Mrs F has said she didn't carry out the transactions in dispute. So, I must give my view on whether I think Mrs F authorised the transactions or not.

All the payments in dispute were made online using the card ending *2765. Mrs F says her old card expired in September 2024, and she never received the new card. However, the physical card was not used to make these payments. But the long card number, the CVV number and expiry date details would've been needed online. This information is also available on Mrs F's app, and I can see these were viewed in her app while logged in from her usual device at her usual IP address in November 2024.

So, whoever made these payments had access to Mrs F's card details – which I accept could've been compromised in many ways – one of which could've been when it was sent to an address Mrs F didn't reside at anymore. However, Santander has also provided evidence that the first payment to each of the merchants in question passed through an additional 3DS security step which was verified via Mrs F's online banking app each time. The evidence shows the verification came from the app on her registered device (the only device registered to her account), and from the same IP address as other undisputed transactions and app activity. So even if someone else had gotten hold of Mrs F's card details, this doesn't explain how the transactions were verified through her online banking app on her phone.

There is evidence that other transactions in dispute passed through an additional 3DS verification in the form of an OTP sent to her registered mobile phone number. This involves an OTP being sent to Mrs F's phone number which is then entered on the payment website to complete the transaction. So again, even if someone else had Mrs F's card details, I have not been provided any evidence to explain how transactions were verified using an OTP sent to Mrs F's phone when she has had possession of her phone the whole time.

I accept there is the possibility that a third party has remote access to her device which has allowed them to authorise the payments in the way discussed above. However, this would only be accessible had Mrs F shared or been tricked into sharing a remote access code with a third party. We asked Mrs F if she had shared any codes or received any suspicious calls, texts or messages recently. Mrs F said she hadn't, and she specifically told us that no one else has had access to her device. So, I've not been able to find a compromise of Mrs F's phone or online banking account which would've allowed these transactions to take place without her authorisation.

I've also noted that Mrs F says she doesn't usually check this account, however the evidence shows she logged into her online banking on 22 November 2024 to make a payment from her Santander account to another account in her name. This payment is not in dispute, so Mrs F accepts she did this herself. And had she not been aware of the transactions in dispute I would've expected her to have flagged this with Santander at this time, as the balance on her account would've then been significantly lower than had been expected.

So overall, I've not been persuaded these transactions were unauthorised and therefore I don't think Santander need to do anything further here.

My final decision

For the reasons outlined above, I am not upholding this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs F to accept or reject my decision before 2 December 2025.

Sienna Mahboobani
Ombudsman