

The complaint

Mrs H 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 case are well known to both parties, so I won’t repeat them in detail here.

In summary, Mrs H says on 14 January 2024 she noticed several payments made from her account to unknown recipients which she says she didn’t authorise. There were several transactions made between 11 January and 13 January 2024, totalling £1,930. Mrs H says she lost her phone in September 2023, and she thinks someone has been able to make these payments using the information from her lost phone. So, she says Santander should refund these payments.

Santander considered Mrs H’s claim and decided not to refund the payments. It says the evidence shows the payments were made from Mrs H’s regular device (used for genuine activity since the theft of her previous phone) via her online banking. So, it says it thinks Mrs H was responsible for making the payments herself.

Our investigator considered all the evidence and information available and decided not to uphold this complaint. Mrs H wasn’t happy 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.

Mrs H says on 14 January 2024 she noticed five payments sent from her account which she didn’t authorise and contacted Santander immediately. Mrs H says she lost her iPhone 14 on 20 September 2023, and she thinks this device, or the information on this device, allowed a fraudster to access her account and make these payments. Mrs H told us that she received a message on her new device three days after her phone was stolen, saying her phone had been found and included a link to its location, which she clicked. She now says she thinks this text was sent by the fraudster. She also provided evidence that she went on a family holiday and provided evidence of a ferry ticket for 2 January 2024, returning on 8 January 2024.

I have considered Mrs H's evidence alongside everything she has said. The dates of the ferry crossing she has supplied are for dates prior to the disputed transactions, and in any case, these were made via her mobile device which she is likely to have had on her anyway. I've also thought about what Mrs H said about the message received on her new device. While it looks suspicious and could've been sent by a fraudster, I am still not persuaded that this allowed a fraudster to make these transactions on her account, I'll explain why.

Mrs H told us that she went to the Apple store the day after she received the text and clicked on the link. She says she showed Apple the text and they reset her device for her. So, I think this would've limited or removed any kind of account sharing or remote access apps. Remote access apps usually also require a passcode to be shared with the third party to grant access, and I've not seen any evidence anything like this happened in this case. And this all took place in September 2023, but the transactions in dispute didn't take place until January 2024. This is not typical of fraud, usually once a fraudster gains access to someone's device or account they act quickly to withdraw or transfer funds as soon as possible. So, it's unusual and unlikely fraudulent activity will take place months after a device or account has been compromised.

I've also considered the evidence supplied by Santander. This shows the transactions were made from an iPhone 13 - which Mrs H has confirmed is the device she has been using since the theft of her iPhone 14 – and this is the same device which had been used for undisputed activity since September 2023. Mrs H said that no-one else has had access to her device or her online banking account. So as the activity in dispute was carried out on Mrs H's device which was in her possession, it seems likely this was carried out by Mrs H herself.

Santander has also provided evidence to show that biometrics were used on this known device to authenticate the payments in dispute. It says Mrs H requested new online banking credentials in October 2023 and this was sent to her in two separate letters by registered mail. These credentials were then used to set up her online banking on her iPhone 13 in November 2023. Since then, the online banking has been used, with no known concerns about unauthorised access.

Mrs H says while she did set-up online banking on her iPhone 13 using the credentials sent to her by post, she didn't set up any biometrics for her banking app. She only set up and used a passcode for her online banking activity. However, the banking audit report evidence shows that for each of the disputed transactions the app was logged in from the known iPhone 13 device using Mrs H's passcode. And then biometrics were used to authenticate each of these payments. Mrs H says no one else had access to her device or knew her passcode. So, there is no explanation as to how someone else could've logged into her banking app on her device and made these payments through her app, even if they had access to the information on her stolen phone. Therefore, I am not persuaded these transactions were unauthorised.

Mrs H says Santander should've identified these transactions as suspicious and their systems should have detected this is unusual activity as she usually doesn't make money transfers from her account, other than to another account in her name. But as I've already said above, I don't think these transactions were authorised. In any event, usually we would expect large payments, perhaps international payments, or payments significantly out of character to be flagged. The payments in dispute were for a relatively low sums and there was no indication that this could have been fraudulent – like incorrect passcode attempts or logins from another country. So, I don't think Santander did anything wrong by not blocking these payments.

While I know this is not the outcome Mrs H was looking for, based on the evidence available

I think it's more likely these transactions were authorised by Mrs H. So, I won't be asking Santander to refund this money.

My final decision

I am not upholding this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs H to accept or reject my decision before 3 February 2025.

Sienna Mahboobani
Ombudsman