

The complaint

Mr L complains that Santander UK Plc (“Santander”) failed to refund transactions he didn’t recognise.

What happened

What Mr L says

Mr L said that his phone was stolen whilst on an evening out with friends on 11 September 2023. He said he reported the theft to the police that same day, but was told that because they were busy, they couldn’t register the theft and he made a written submission two days later (13 September).

Mr L explained that his phone didn’t have a “sim” card in it as he used another one for that purpose, but the stolen phone did have his bank app and debit card with it. He called Santander straight away and reported the theft and several unrecognised transactions to a crypto trading platform I’ll refer to as “C”.

Mr L received a temporary refund of some of the unrecognised transactions, and his card was replaced. Mr L said he had difficulty making a report to Santander and tried several times to send them details about the loss. Mr L said that Santander then took back those temporary refunds which caused him financial problems because he had to arrange for other funds to be transferred into his Santander account.

Mr L complained to Santander who investigated the issue. They later sent him their final response letter explaining that their evidence showed the payments were made using a known IP address and the payments had been authorised “in-app”. They held Mr L liable for the transactions he’d disputed but acknowledged that their handling of the dispute was incorrect. They credited Mr L’s account with £50 compensation.

Mr L was left unhappy with how his situation had been handled by Santander and brought his complaint to the Financial Ombudsman Service for an independent review.

What Santander say

Santander received notification from Mr L about the loss of the phone and their reports first record this on 11 September 2023. They issued a temporary refund for some of the payments and conducted their own investigation.

They concluded that it was unlikely the transactions were carried out by a third party due to the technical evidence of how the payments were authorised and how the app was used.

They accepted they could have been clearer when they spoke with Mr L and provided a small payment to him to recognise this failing in customer service.

The investigation so far

After receiving Mr L’s complaint, both parties were asked to provide information about the situation. Mr L was able to confirm his version of events and in summary added:

- He’d suffered other compromises of his Santander account over recent years.
- He wanted a refund of the unrecognised transactions and £300 compensation.

- He tried to remotely wipe his phone but was unsuccessful.
- Other accounts had evidence of a third party attempting to access them.
- He'd received refunds from another bank.
- His phone was protected by a "pattern sign" which could have been observed during the evening out.
- His Santander banking details were contained in a file on his phone.

Santander provided information concerning their investigation including system information showing how the transactions had been made. In summary this showed that:

- The first payment to C had been made on 8 September.
- Mr L had used biometric security to operate his banking app after the date of the theft.
- There was no evidence of a change of login credentials (which would be the case if new biometrics were introduced).
- There was a consistent IP address used both prior to, during and after the date of the theft.
- Santander acknowledged that the handling of Mr L's dispute was unsatisfactory and made a payment of £50.

After reviewing the evidence, the investigator upheld Mr L's claim for a refund including a payment for interest but thought that Santander's payment for their customer service was reasonable.

The investigator commented that they weren't satisfied that Santander had provided sufficient evidence to show Mr L authorised the payments. They said shoulder surfing couldn't be discounted for how someone could access the phone. It would then be possible to access the banking app to confirm the payments.

Mr L accepted the investigator's outcome, but Santander didn't and continued to argue that:

- Biometrics were used to authenticate the payments and there was no evidence they had been changed.
- If unauthorised third parties had been responsible, they also had access to other funds in another account which they didn't use which would be unusual.

Because no agreement could be reached, the complaint has now been passed to me for a decision.

As part of my own investigation, I asked Mr L to confirm some details based on the payment data because Mr L's original dates that he reported seemed to indicate some transactions to C happened before his phone was reported lost.

Mr L said that he now believed the date of loss was 10 September and he called the following day (rather than 11 September and calling the same day). Mr L also confirmed he didn't have an account with C. He also believed his biometrics could be used by those that stole his phone.

Mr L explained that he used a type of IP arrangement that meant his IP address was "static", explaining why it remained the same although he was unable to provide evidence of this as he no longer had his phone or the relevant account details.

I issued my provisional findings on the merits of Mr L's complaint on 31 December 2024. In my provisional findings, I explained why I intended not to uphold Mr L's complaint and

offered both sides the opportunity to submit further evidence or arguments in response. An extract of that decision is set out below and forms part of this final decision:

“What I’ve provisionally 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.

The relevant law surrounding authorisations are the Payment Service Regulations 2017. The basic position is that Santander can hold Mr L liable for the disputed payments if the evidence suggests that it’s more likely than not that he made them or authorised them, but Santander cannot say that the use of the payment card for online payments conclusively proves that the payments were authorised.

Unless Santander can show that consent has been given, it has no authority to make the payment or to debit Mr L’s account and any such transaction must be regarded as unauthorised. To start with, I’ve seen the bank’s technical evidence for the disputed transactions. It shows that the transactions were authenticated using the payment tools issued to Mr L.

It’s not my role to say exactly what happened, but to decide whether Santander can reasonably hold Mr L liable for these transactions or not. In doing so, I’ll be considering what is most likely on a balance of probabilities.

It’s Mr L’s case that after his phone was stolen, his account was compromised. His payment card was used to make transactions to C after those payments were confirmed through the use of the banking app. Santander believe that Mr L himself was responsible, primarily based on the audit data related to the use of the phone.

When I’ve examined the information provided by both parties, the transaction data supplied by Santander shows the first payment to C was made on 8 September 2023. That payment was made using Mr L’s phone which hadn’t yet been stolen according to his (updated) information.

Mr L said he didn’t have an account with C. But it seems unlikely that an unidentified third party would set up an account with C and send money using Mr L’s account. If they had somehow managed to gather the required information and access to his phone (notwithstanding the use of biometrics), there wouldn’t then be a need to steal it.

Santander didn’t have any evidence of a change of biometrics, which would be the case if a thief wanted to use their own. Given that the transactions started some days before Mr L reported his phone was lost and they used biometrics, it seems unlikely they were carried out by anyone else.

I’ve also considered the issue of the IP address data and whilst I have some questions about Mr L’s arrangement that he described; I don’t think for the purposes of this complaint that the IP data is particularly relevant.

What is relevant is that the transactions reported by Mr L first took place some days prior to the reported loss of the device. Mr L has already amended the dates of the events from his original reports to the bank, the police and our service, but they still don’t account for how payments to C were made by someone other than Mr L.

Given the available evidence, I currently think it’s more likely than not that Mr L was responsible for the disputed payments from his account, and it was both fair and reasonable for Santander to hold him liable.

My provisional decision is that I currently intend not to uphold this complaint.”

I invited Mr L and Santander to give me any more evidence and information they wanted me to consider before issuing my final decision. Santander didn't have anything further to add about the complaint. Mr L continued to say that the payments had taken place after his phone was stolen. Mr L believed that Santander had been given preferential treatment when supplying information and they hadn't given him the relevant evidence.

Mr L was provided with copies of evidence that had been relied on in respect of the disputed payments. Mr L replied and stated that the date of the transaction was 9 September (taken from his app) and not 8 September (taken from Santander's audit records).

Mr L believed Santander hadn't provided the evidence to him when they should have done and he believed that Santander didn't have permission to share all his data with our service. He continued to argue that biometrics can be bypassed and thought that some of Santander's evidence had been fabricated.

Mr L wanted another review of his complaint as he believed it was biased against him.

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.

Having done so, and as neither party had anything further to add that would change my provisional decision, I see no reason to reach a different conclusion. So, this final decision confirms the findings set out in my provisional decision.

I will address the points raised by Mr L:

- Santander's data was provided at the start of the complaint raised by Mr L for which he provided appropriate permission to our service to obtain and consider the relevant information from the appropriate parties (here Santander).
- There's no evidence that any of the information provided by Santander was fabricated.
- There's no evidence to support Mr L's belief that his biometrics were somehow bypassed.
- The evidence from Santander's audit showed the first transaction to C was on 8 September and not 9/10 or 11 as previously alleged by Mr L.

Mr L has been unable to explain how the transactions he's disputed to C were first made prior to the theft of his phone. He's changed the dates he lost it on several occasions and I'm unconvinced about the accuracy of his information. As I've already mentioned, it's unlikely that a phone thief would set up payments to C before stealing his phone. Without a reasonable explanation that can account for those earlier payments to C, it just isn't plausible that anyone else but Mr L was responsible for those payments. Even if I was to accept Mr L's latest version of events regarding the dates, I'd likely still conclude that these transactions were carried out by him given the lack of change in the biometrics that were used as part of the payment process.

So, having considered all the evidence and points raised by Mr L, I'm satisfied that, on an impartial review of the evidence, that Mr L was more likely than not responsible for the transactions he's disputed. It was both fair and reasonable for Santander to hold him liable for these payments.

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 L to accept or reject my decision before 24 March 2025.

David Perry
Ombudsman