

The complaint

Miss K complains that Santander UK Plc (“Santander”) failed to refund transactions she didn’t recognise and added an overdraft to her account without her permission.

What happened

Miss K noticed a number of transactions had been made from her account that she didn’t recognise. She contacted Santander about them and reported numerous unrecognised payments to two different merchants. I’ll refer to them as A and T. Miss K also noticed that several overdraft applications had been made (increasing the amount on each occasion) and an attempt to apply for a loan (which was declined).

Santander said that Miss K had a genuine relationship with A and she should approach them about the payments she was disputing – and a number of refunds had been applied to her account by A.

Santander looked into the situation and initially investigated only a few transactions reported by Miss K (related to T). Later, Miss K complained to Santander about the investigation and the lack of clarity surrounding the disputed payments/the overdraft and the loan. She believed her account had been taken over by persons unknown, probably through some sort of “hack” of her account and phone.

Santander investigated Miss K’s complaint but didn’t think there was anyone else involved. They couldn’t find any evidence of a third-party accessing Miss K’s account and their audit data indicated that Miss K’s genuine mobile phone was used to confirm the payments.

Miss K was left unhappy with her situation and how Santander had handled her issue. She brought her complaint to the Financial Ombudsman Service for an independent review. An investigator was assigned to look into what had happened and both parties were asked for information about the situation.

Miss K was able to say that:

- A large number of disputed transactions took place using her Santander account.
- She confirmed she’d made a single payment with the same merchant, but not the rest of them.
- Miss K was severely ill at the time and not aware of any of the transactions being made from her account.
- She knew nothing about the overdraft or loan applications made in her name.
- She’d had other loan applications made to other companies without her permission.
- She believed that she was the victim of a “hack” that had allowed someone else to use her account.

- IP addresses are “spoofed”.
 - Note: IP addresses are a means to identify physical locations that online transactions are connected to and can be the actual physical location or other locations connected to the provider of the data services.
- She never lost her phone or allowed anyone else to use it. Nor did she divulge any of her security/ card details to anyone else. She also confirmed she hadn’t been asked for any of this type of information by anyone.
- Miss K was unable to provide any evidence from her phone provider – but said that it was difficult to provide evidence of a “hack”.
- Miss K also complained that she’d been laughed at by a Santander employee when she reported the disputed transactions.

Santander provided details of their own investigation and audit data concerning how the disputed transactions had been carried out. A copy of the call was also provided related to the complaint from Miss K about treatment she received by an employee.

In summary, Santander’s information showed that:

- Miss K’s own device (mobile phone) was used to confirm the payments using additional security steps.
- That same device was used to apply for the overdraft and subsequent increases.
- IP address data showed Miss K’s device being used from the same location as non-disputed transactions were made from.
- There was no evidence of any third-party involvement.
- Miss K had made a payment to her credit card provider using her device around the same time as some of the disputed transactions.

After reviewing the evidence provided by both parties, Miss K’s complaint wasn’t upheld. The investigator commented that:

- The transactions were authenticated using Miss K’s registered phone after receiving additional security codes. The IP address indicated the same location was used for other undisputed transactions.
- There’s no evidence to show her phone was “hacked”.
- Even if it was “hacked”, there’s no explanation how someone could obtain the necessary security information known only to Miss K.
- There’s no evidence that Miss K was mistreated when she called Santander.

Miss K disagreed with the investigator’s outcome and in summary said:

- She maintained she had nothing to do with the disputed transactions.
- Santander failed to properly investigate her complaint.

- There was evidence of the overdraft being increased without her consent.

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.

The relevant law surrounding authorisations are the Payment Service Regulations 2017 and the Consumer Credit Act 1974. The basic position is that Santander can hold Miss K liable for the disputed payments if the evidence suggests that it's more likely than not that she made them or authorised them.

Santander can only refuse to refund unauthorised payments if it can prove Miss K authorised the transactions, but Santander cannot say that the use of the card and online payment details 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 Miss K'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 Miss K. I'll now need to consider the information provided by both parties to determine whether there's sufficient evidence to hold Miss K responsible for the disputed transactions or not.

Miss K's complaint is that she wasn't responsible for these payments, whilst it's Santander's position that there's no evidence anyone else was involved.

Having examined the evidence provided by both parties, it's apparent that the disputed payments were made using the details from Miss K's debit card and confirmed after a separate procedure was carried out using Miss K's banking app from her phone. In order to carry out these transactions, the user needed access to Miss K's phone, her codes to access the phone, plus her codes to access her mobile banking app. None of which were divulged to anyone else.

On the face of it, it seems unlikely that an unidentified third party could obtain the necessary information with which to access her mobile banking app and confirm each payment made to T. Also, the IP address data is consistent with other non-disputed uses, indicating the same user in the same location was responsible for these disputed transactions.

I understand that Miss K has said that these IP addresses can be "spoofed" (meaning in this context to show a different location than the genuine one). I've thought about that and whilst it's technically possible, I doubt it's the answer to what happened here. That's because there's no other evidence to show how the private security information could have been obtained and there's also evidence to show that Miss K made a payment from her Santander account using her mobile banking around the same time some of the disputed transactions were being carried out.

Specifically, that means Miss K was using her account when she said she was unaware of the activity on her account. The audit data doesn't support her assertion that she wasn't using her mobile banking around the same time as the reported activity on her account and the IP address data is consistent.

I've also looked at the overdraft applications which Miss K denied being involved in. The

evidence from Santander shows that Miss K's mobile banking was used to apply for it and the additional increases, each time authenticated by the confirmation of a One Time Passcode sent to her mobile phone number registered with Santander. So, the evidence here is that it wasn't an unidentified third party responsible for applying for the overdraft.

There was also a loan application which was declined, so I won't consider this any further as there was no financial impact on either Miss K or Santander. I have seen evidence from Miss K that other loan enquiries were made, but as these were to other providers, I haven't further considered them in this complaint. I also don't think they support Miss K's case that she wasn't responsible. That's because, on balance, and after an objective assessment of the available evidence, I'm satisfied that Miss K was more likely than not responsible for these transactions and the overdraft applications. It was both fair and reasonable for Santander to hold her liable for them.

I've also listened to the call where Miss K alleges she was treated poorly. Having done so, I couldn't hear anything that could be interpreted as being laughed at. The conversation was carried out by the Santander employee based on the information he was aware of at the time and he logged Miss K's dissatisfaction when she was told they weren't supporting her application for a refund. It was apparent that not all of Miss K's points had been investigated at that point, but this was later carried out by Santander and communicated to Miss K.

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 Miss K to accept or reject my decision before 30 January 2024.

David Perry
Ombudsman