DRN-4359008

The complaint

Miss W and Mr W complain that Santander UK Plc failed to refund transactions they didn't recognise.

What happened

As Miss W was primarily involved with the disputed transactions, I'll generally refer to her to make reading this decision easier.

Miss W was alerted to unusual activity on the joint account she held with Mr W. She'd received three One Time Passcodes (OTPs) relating to transactions being made through the account.

Miss W then went on to her mobile banking app using her registered phone and found that three payments had been taken from the account leaving less than a pound balance. Miss W asked Santander for a refund because she didn't recognise these payments or authorise them. Miss W was told by Santander that the payments were confirmed by the use of OTPs sent to her registered device (mobile phone) and because Santander received the appropriate response, the payments were completed.

Miss W strongly denied making these payments and complained to Santander about the lack of refunds and their treatment of her and Mr W whilst they were trying to deal with the situation. Miss W and Mr W explained that they'd had messages from other providers including their email provider, that unknown devices had logged into their accounts or attempts to obtain private data about them had been attempted.

Santander investigated the complaint and recognised they let both Miss W and Mr W down with their service. In their final response, Santander apologised for causing unnecessary distress and inconvenience. They credited their account with £40 as a gesture of goodwill. Santander didn't accept that they'd made an error concerning the disputed transactions and continued to hold both Miss W and Mr W liable for them. Santander said that they'd review the complaint again if evidence was obtained showing how their information could have been compromised (banking logon details and access to the OTP).

Unhappy with how Santander dealt with their complaint, Miss W and Mr W brought it to the Financial Ombudsman Service for an independent review where it was looked into by one of our investigators.

Both parties were asked for information about the complaint and Miss W and Mr W provided:

- Screenshots showing OTPs and requests to reset passwords.
- Confirmation that their email had been accessed by an unknown device.
- Evidence that a different mobile phone number had been associated with one of their accounts (not Santander).

It's their case that their account was compromised, and the payments taken from it without their permission. Miss W pointed out that the IP address data was different to that usually used by them and the device used to make the payments wasn't theirs. They also pointed out that this account wasn't used for payments of this sort and that they didn't have any relationship with the merchant who received the payments (a betting company).

Miss W went on to say that her phone was protected by biometrics and a passcode that wasn't known to anyone else and her bank account was also protected through biometrics (for mobile banking) and a passcode. She said that no one else could have seen her phone at the time of the disputed transactions and the OTPs weren't given to anyone. She confirmed she hadn't been approached to reveal any sensitive information about her account. She was genuinely puzzled how these payments could have been allowed to leave her account.

Santander provided system data about how the account was operated and the audit of what happened at the time of the disputed transactions. In summary this showed that:

- A login from the internet was made to the account and "re-access" requested requiring an OTP to be sent to Miss W's mobile phone, which was successfully completed.

- Access to "Open Banking" was provided through a third-party merchant on behalf of the betting merchant. This required knowledge of Miss W's online banking details in order to log in to the account.

- Additional OTPs were sent to authorise each of the three payments – all to Miss W's mobile phone.

- Miss W successfully logged on to her account via her mobile device, shortly after the three transactions had been completed.

- There's no explanation how the necessary information and OTPs could have been obtained by someone else.

After reviewing the evidence, the investigator recommended no further action be taken by Santander and didn't uphold Miss W and Mr W's complaint. It was commented that:

- Miss W's phone was protected via biometrics and a password which no one else had access to.

- No details were shared with anyone else, and they weren't written down anywhere.

- The OTP's received weren't shared with anyone.

- The IP address was different to that usually used by Miss W and Mr W, although this wasn't conclusive evidence that someone else was responsible.

- Miss W was able to successfully log on to her account shortly after the disputed transactions were completed using her mobile device which contained the OTPs. There's no explanation how they could have been obtained by anyone else.

- Santander's payment of £40 was a fair way to recognise their level of customer service experience by Miss W and Mr W.

Both Miss W and Mr W disagreed with the outcome and said that:

- They reiterated the different IP address and unknown device used to make the payments.

- They believed the time between the OTP being sent and the authorisation didn't allow time for the messages to be read and checked.

- Evidence was supplied showing unauthorised access to their accounts (email and others).

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

Miss W and Mr W wanted the issue of the disputed transactions reviewing, so I haven't further considered the response by Santander to the customer service aspect of the complaint.

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

Santander can only refuse to refund unauthorised payments if it can prove Miss W authorised the transactions, but Santander cannot say that the use of internet (open) banking 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 W and Mr W'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 W. I'll now need to consider the information provided by both parties to determine whether there's sufficient evidence to hold Miss W and Mr W responsible for the disputed transactions or not.

The disagreement between the parties centres around whether the joint account was compromised by unknown third parties to allow them to make the three disputed transactions or whether the evidence points towards Miss W being liable herself.

I recognise the evidence supplied showing other devices (mobile phones) having access to their email account and the account of their phone provider. It's apparent that other unknown parties were able to access these accounts for a short while before they were secured.

There's no evidence or explanation about the specific information available from these accounts, for example what details were kept on them. Neither Miss W nor Mr W have said they kept their banking details on these accounts, so it's difficult to see how someone could obtain the necessary information to enable them to log into the account.

Regarding the OTPs, I'm unable to see any explanation how they could have been obtained by other parties because they were sent to Miss W's registered phone and responded to. A number of these OTP's were provided, including those that needed extra steps in order to log in to the account using the internet.

The “Open Banking” referred to above relates to how access was provided between the Santander account and the betting account. This required the private security information for Miss W’s account to be entered and permission given to take payments for the betting merchant. As I’ve already mentioned, I haven’t seen a plausible explanation how this information could have been obtained, despite the evidence of the email breach.

The IP address data referred to in this complaint is different to those addresses usually used by Miss W and Mr W. It can be an indicator of misuse, but it’s also not always conclusive and here, there are various addresses scattered throughout the UK which make it difficult to establish any particular pattern – one way or the other.

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.

I examined the timing issue mentioned by Miss W and it’s apparent from the audit information that those OTPs (for the disputed transactions) were each responded to. There was a gap of between about 40 – 50 seconds between them being sent and the response received by Santander. I don’t think this is a particularly unusual time window or noteworthy.

I’ve thought whether Miss W’s phone itself could have been taken over by a third party which could account for the OTP’s being obtained. But, if that were the case, it’s unlikely that she herself would have continued access, which wasn’t the case here because she was able to continue to use it and retained access to her account.

I also considered why an unknown third party would choose to use a betting merchant if they had access to the online banking account? It’s the case here that in order to give permission for “Open Banking”, the online bank account was accessed using Miss W’s credentials and the OTP from her phone. If I accepted that this was done by an unknown third party, I’d question why they used those funds with a betting company when it would have been fairly straight forwards to send them to another type of account where they could take those funds and use them rather than gamble with them.

So, I think there’s a question why someone would go to the trouble of obtaining Miss W’s details and somehow get the OTPs’ to then use them with a betting merchant, rather than take the funds themselves.

Overall, and whilst I’m sure that both Miss W and Mr W will disagree with me, I think on balance, after an objective review of the evidence, that it’s more likely than not that Miss W was responsible for making these transactions herself or allowing someone else to carry them out with her permission. I think it's both fair and reasonable that Santander held them liable for the payments and I won’t be upholding this complaint.

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 W and Mr W to accept or reject my decision before 29 December 2023.

David Perry
Ombudsman