DRN-4874954

The complaint

G complains that Santander UK Plc failed to refund transactions they didn't recognise.

What happened

G are represented here by Mr H. I'll mainly refer to him throughout for ease of reading.

Mr H explained that he was at a party with friends and had been drinking. At some point he gave his unlocked phone to a friend as he thought he was ordering some more supplies for the party.

Mr H said he provided access to his phone (he thinks by using his biometrics) which his friend kept for a little while. Sometime later, Mr H realised that two transactions had been made from G's account using the faster payment process. Mr H later told our service that he wasn't aware that the banking app for G was open and logged into. He also said at some point he saw the Santander logo and was suspicious after being asked to provide his fingerprint. He said he was asked later to again provide his fingerprint and refused.

Mr H approached Santander about the situation and asked for a refund. Santander made enquiries about the payments and were later able to return one of them. Santander concluded that Mr H was himself responsible and declined to make a refund of the remaining disputed transaction. Mr H complained and Santander investigated the circumstances. They continued to believe Mr H was responsible and didn't offer any further refund.

Mr H (through G) were left unhappy and brought their complaint to the Financial Ombudsman Service for an independent review. An investigator was assigned to the complaint and asked both parties for information about the circumstances.

Mr H was able to confirm his version of events and added that:

- one of the people who used use his phone wasn't known to him.
- He thought he was authorising a payment for food delivery.
- Mr H also said that the Santander app was being tested at the time and it had now changed how it worked.
- He didn't have any passcodes stored on his phone.
- He wasn't aware of any One Time Passcodes (OTPs) sent to his phone.
- He believed only biometrics could be used to set up and authorise new payments.
- He reported the matter to the police.

Santander provided audit data, calls and information relating to their own investigation, in summary this showed that:

- The two payments were set up using the banking app.
- Passcodes were used to login to it.
- The payments were subject to a secondary process (OTP) which was authorised within the app.
- Santander believed Mr H authorised the payments.
- Santander had also said Mr H had logged on to his mobile app using biometric security but later amended this to using his passcode.

The investigator discussed the regulations and terms of the account about keeping the account details secure (including biometrics). It was argued that Mr H had beached those terms and was grossly negligent when he allowed others to use his account which enabled them to make transactions. His complaint wasn't upheld.

Mr H, on behalf of G disagreed and argued that:

- He implicitly trusted his friend.
- He said the app only had the option to use biometrics.
- Biometrics only prove the person was "bodily present".
- Santander have provided conflicting information.
- The app wasn't secure.
- He wasn't negligent.
- He can't exactly remember what had happened.

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.

Mr H has argued that the app was insecure, allowing his biometrics to be used to set up transactions that he didn't agree to. It's been argued that he was grossly negligent when he gave his unlocked phone to his friend and then used his biometrics to assist with processing the payment.

It's the case here that Mr H was at a party and he himself says his memory of what happened is unclear. Mr H says he gave his unlocked phone to a friend to make certain purchases for delivery to the party.

What in fact happened was that two payments were set up to new bank accounts using the Santander app after it was accessed using the passcode issued to G (Mr H). Additional security steps were carried out within the app (OTP) to authorise the two bank transfers.

These payments could only have been carried out after gaining access to the banking app. Mr H has argued about the security of the app and some of Santander's evidence refers to "touch id" (fingerprint), although they later provided some deeper audit data showing the passcode for the app was used.

I acknowledge Mr H's belief that the app was insecure, but Santander's evidence shows information known only to him (either the passcode or biometrics) was used to access the app. This is a typical way for such apps to be accessed, so I don't think it's accurate to say the app was unprotected.

Whether it was biometrics or the passcode that Mr H used is essentially irrelevant here. What is relevant is that either the passcode or Mr H's biometrics were provided by him to open the banking app – neither of which was known or useable by his friend. From that point on his friend was able to use the account. Mobile banking data shows the account was open for about ten minutes, which seems to fit with Mr H's belief they had his phone for some time, enabling them to deal with the additional security steps generated by Santander whilst they had access to the app.

Mr H says he noticed the Santander logo at some point, although he was expecting to make a purchase for online deliveries (which is a markedly different process).

A payment service user's obligations are set out in the **Payment Service Regulations 2017 (PSRs)**.

Regulation 72 says that a consumer must:

- take all reasonable steps to keep the personalised security credentials relating to a payment instrument safe.

Regulation 77 goes on to say:

Payer or payee's liability for unauthorised payment transactions

> (3) The payer is liable for all losses incurred in respect of an unauthorised payment transaction where the payer—
>
> > (b) has with intent or gross negligence failed to comply with regulation 72 (obligations of the payment service user in relation to payment instruments and personalised security credentials).

Santander's terms for this account state:

What are your personal security details?

These are the security processes we set up with you and the credentials we give to you or that you choose. These include things like:

- *Passwords, PINs, security codes and memorable information*
- *Your fingerprint, voice, face ID or other biometric information*

It's important that you keep your card, chequebook (if you have one), and personal security details safe to prevent fraud and protect your account.

What you and your authorised persons shouldn't do

- *Don't share your personal security details with someone else, including your employees.*
- *Don't give your chequebook or card (or any device it's stored on) to someone else, including your employees.*

Unauthorised payments

What's happened?
A payment's made from your account that wasn't authorised by you, or someone allowed to make payments from your account.

Will we refund you?
It depends. If you didn't keep your card or personal security details safe as we told you to, either intentionally or very carelessly we won't refund you.

So here, the various terms and regulations provide a framework for how the security details (including passcode, device and biometrics) are required to be handled by Mr H.

S 77 is of particular relevance here as it introduces a test for "intent or gross negligence"

The test for gross negligence is based on what a "reasonable person" would have done in the same situation. Mr H would have to have acted with a*"… very significant degree of carelessness"* which is how the Financial Conduct Authority (FCA) define gross negligence.

Mr H's version of events is hazy, he confirmed he couldn't really remember, in detail, what went on at the time he passed his phone to his friend.

Mr H said he was assisting with a payment for a delivery for the party. Usually, such transactions would take place on the merchants own website using a credit or debit card to settle the payment. That's quite different to what actually happened, here Mr H allowed his friend access to his Santander account (and saw their logo at some point), a very different financial platform and left them with his phone for a considerable period of time.

Given the length of time they had his phone and the knowledge they'd been on the Santander app, I think Mr H's apparent lack of concern or action to retrieve his phone led to the loss of the funds from G's account.

So, on balance, I think that Mr H failed to comply with:

- The PSRs relating to account and device security, leading to the loss of funds (72 & 77 refers); and

- the terms of his account by failing to keep his security credentials safe.

I say that because Mr H:

- allowed others to use his unlocked phone without any supervision.
- He opened his Santander app using his biometrics or passcode.
- He'd seen the Santander logo at some point.
- He left the phone with them for a long time and others were able to use it, including passing Santander's additional steps to set up the faster payments.

In summary, I think that Mr H's actions led to the compromise of the account by others, enabling them to make payments (to themselves). I'm satisfied that Mr H's actions were in contravention of the terms that were agreed to for G's account and meet the test for gross negligence. I don't think his actions were what a reasonable person would have done in the same situation. He effectively bypassed Santander's app security, preventing them from protecting the account. It follows that I don't think it would be fair or reasonable to ask Santander to make a refund.

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 G to accept or reject my decision before 28 November 2024.

David Perry
Ombudsman