

The complaint

Miss P complains Santander UK Plc (“Santander”) closed her account, and then unfairly applied an adverse fraud marker against her.

Miss P is represented by her mother. Where possible, and to keep things simple, I will refer to Miss P in my decision.

What happened

Around £1,700 was credited into Miss P’s Santander account on 15 November 2019. This money was then spent over the next few days through a combination of ATM withdrawals, CHIP and PIN; and contactless transactions.

All the transactions are well known to both parties, so I won’t list them in detail here.

On 18 November 2019, three days after the above funds had come into Miss P’s account, a third-party bank – who I will know refer to as Bank A – spoke to Santander. Bank A said a second transfer from its customer had been attempted to Miss P’s account. It said that this was from the same account as where the £1,700 was sent from.

Bank A suspected an unauthorised individual had impersonated its customer by having transferred funds to Miss P’s Santander account – and then tried to do so again.

Santander blocked Miss P’s account and called her. Miss P said she did not recognise the large transfer that credited her account three days earlier. Santander say the call disconnected prematurely. And when it called Miss P back there was no answer.

Two days later, Santander wrote to Miss P telling her it has been attempting to contact her at that it had temporarily blocked Miss P’s account until it can discuss matters with her.

Miss P called Santander on 25 November 2019 and reiterated she did not recognise the large sum that came into her account ten days before. In early December 2019, following a review, Santander sent Miss P a letter saying it had decided to close her account with immediate effect.

Santander also loaded a CIFAS fraud marker against Miss P under the category of ‘misuse of facility’. Miss P tried to open a new bank account with another bank but was refused. Miss P and her representative then complained to Santander.

In summary, Santander said the following in its final response:

- As its attention was drawn to a potentially fraudulent payment on Miss P’s account, it had no alternative to suspend the account until she was able to provide information about the source, and her entitlement to the funds
- Based on the information given, Santander decided to withdraw Miss P’s banking facilities. Santander had done so in accordance with its terms and conditions

- Organisations will review any information held with fraud prevention agencies, and they will make decisions based on their own policies and procedures. Santander has no power over any decisions other financial institutions make.

Unhappy with what Santander said, Miss P referred her complaint to this service. One of our investigator's then looked into the matter. In short, they found:

- The transactions made on Miss P's account following the £1,700 being paid in were all authenticated. They had seen records which showed the genuine CHIP, card and smart-phone payment were read - and the correct PIN entered
- It appears Miss P has authorised - or given someone else consent – to carry out the transactions made from her account which dispersed the fraudulent funds. That's because:
 - Miss P told this service she had her card in her possession. But said she didn't to Santander's branch staff. This questions Miss P's credibility
 - Miss P said no one knew her PIN and she had never lost it. There was also quite a gap between when Miss P says she genuinely used her card and PIN. So there doesn't seem to be a point of compromise for someone to have seen Miss P's PIN
 - It's unlikely an unknown fraudster would have taken her card and then returned it to her without her knowing
 - Santander's records show Miss P's online account was logged into several times between the time the fraudulent funds come in and they were spent. So its difficult how she wasn't aware of the activity, and why she didn't do anything to prevent it
 - After listening to the calls, it's most likely Miss P and the person that called Bank A impersonating its customer to make a payment, were the same person
- Santander have acted in line with its terms and conditions when deciding to close Miss P's account with immediate effect
- Santander has done enough to show the CIFAS marker was recorded correctly

Miss P and her representative were unhappy with what our investigator said. They wanted to listen to the call our investigator said showed Miss P called Bank A and pretended to be the victim to release funds to her Santander account.

Our investigator did this. Miss P and her representative don't agree this is her and have asked for an ombudsman to decide the complaint.

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.

And having done so, I've decided not to uphold this complaint. I know this will disappoint Miss P, so I'll explain why.

Account restrictions and closure

Santander has important legal and regulatory obligations it must meet when providing accounts to customers. These obligations are ongoing, so do not only pertain to when an account is opened.

To comply with its obligations Santander may need to review an account and/or restrict its customer's access. If Santander didn't comply with its obligations it could risk serious sanction. In order to meet these requirements, Santander is entitled to ask a customer for more information about how they use their account, including payments which are made into an account.

Having looked at all the evidence, I don't believe it was unreasonable in the circumstances for Santander to block Miss P's account and ask her for information relating to activity on the account. So, whilst I accept this matter would have caused Miss P inconvenience, I can't say Santander treated her unfairly when it blocked her account.

A few weeks after restricting Miss P's bank account, Santander took the decision to close it. A bank is entitled to close an account just as a customer may close an account with a bank. But before a bank closes an account, it must do so in a way, which complies with the terms and conditions of the account.

The terms and conditions of the account, which Santander and Miss P had to comply with, say that it could close the account. The terms go on to explain what those circumstances are, and when Santander can close it immediately.

Given the information presented to me by Santander, and other relevant parties; and having looked at the wording of the applicable terms, I can't say Santander acted unfairly in closing Miss P's account with immediate effect. I understand its concern.

So it follows that I'm satisfied Santander was entitled to close the account in the way that it has done.

CIFAS marker

I've moved on to consider the loading of the CIFAS marker.

The marker Santander have filed with CIFAS is intended to record there's been a 'misuse of facility' – relating to using the account to receive fraudulent funds.

In order to file such a marker, Santander's not required to prove beyond reasonable doubt that Miss P is guilty of a fraud or financial crime, but they must show there are grounds for more than *mere suspicion* or concern. CIFAS says:

- "There must be reasonable grounds to believe that an identified fraud or financial crime has been committed or attempted; [and]
- The evidence must be clear, relevant and rigorous such that the member could confidently report the conduct of the subject to the police."

What this means in practice is that a bank must first be able to show fraudulent funds have entered Miss P's account, whether they are retained or pass through the account. Secondly, Santander will need to have *strong* evidence to show the consumer was deliberately

dishonest in receiving the fraudulent payment and knew it was, or might be, an illegitimate payment.

A marker shouldn't be registered against someone who was unwitting; there should be enough evidence to show deliberate complicity. So, I need to consider whether Santander has enough evidence to meet the standard of proof and load a marker for misuse of facility with CIFAS.

Miss P said she doesn't recognise the large payment that entered her account in November 2019 for around £1,700. Having looked at the account records Santander have given me, I note these funds were pretty much spent within three days of them entering the account.

As I've said above, they were spent through a combination of ATM withdrawals, CHIP and PIN and contactless transactions. I'm satisfied from Santander's technical evidence that Miss P's genuine card and PIN were used to make the transactions. That's because they show the genuine CHIP was read, and where applicable, a PIN number was entered to carry out the transactions. Few of the payments were made using a payment facility on a mobile phone.

Miss P has told this service that around the time of the fraudulent funds entering her account she tried to withdraw money using her debit card but had problems with this. As a result she went into a Santander branch to tell them and a replacement card was ordered. She says her mother advised her to cut her previous card into pieces and throw it away.

I note from Santander's internal records Miss P said she didn't have the card in her possession when she went into branch. This sounds discrepant with what she's told this service. But based on what Miss P has told us, and given this is what's been said most frequently, I'm persuaded the debit card which was used to carry out the transactions was in Miss P's possession. After all, she says her mother told her to go straight to the branch when she had problems with the card.

Miss P's representative suggests the card may have been cloned. But I think that's highly unlikely. That's because based on what our service has seen, and the industry guidance available to us, we have yet to see a complaint where the CHIP on a card has been cloned. So I'm satisfied Miss P's genuine card was used.

Miss P says she hasn't written her PIN down or shared it with anyone other than her mother. So because of that, and as the genuine card and PIN were used to make payments that dispersed the fraudulent funds, I find it difficult to understand how these payments happened without Miss P's involvement or knowledge.

And, given the card was in Miss P's possession, I find it even more unlikely that someone unbeknownst to Miss P took her card, carried out all these transactions, and then returned it without her knowing.

Santander have given me screenshots of Miss P's online login records. Having looked through these, I note that there are around thirty logins between the 15 and 18 November 2019. As I understand it, some of these also required 'touch ID' to login. Miss P has said she completed the mobile logins.

Miss P has said she suspected her account was being 'hacked'. That said, and given the online logins, I find it very unusual Miss P would have seen an unexpected large sum enter her bank account, and then see it quickly get spent without reporting this with any urgency to Santander.

It was only when Santander called Miss P that she confirmed she didn't recognise the amount. I also find it difficult to understand why Miss P called Santander a week later to follow up on the matter and not any sooner given the seriousness of what was happening.

Miss P says she couldn't have carried out the transactions because they occurred in locations that were far away from where she lived. She's also sent in information she says shows she was in college.

It's not entirely clear if Miss P was in college or work placement, given she's said that's where she was when her card wasn't working properly. But I don't think that makes much difference to the outcome of this complaint. I say that because somebody else, authorised by Miss P, may have carried out these transactions.

It follows, for the reasons I've explained above, that I'm satisfied Miss P, or someone she authorised, carried out the transactions which spent the fraudulent funds.

Importantly, I know need to consider if Santander has fairly loaded the CIFAS marker to Miss P.

To that end, I'm satisfied Santander and Bank A have given me enough information to conclude fraudulent funds entered Miss P's account. I'm also satisfied, from what I've said above, that I've seen strong enough evidence to show Miss P was deliberately dishonest in receiving the fraudulent payment and knew it was, or might be, an illegitimate payment.

To have reached this finding, I need to be satisfied that the 'evidence must be clear, relevant and rigorous such that the member could confidently report the conduct of the subject to the police' – and I think it is.

Miss P will note I haven't said anything about the call from Bank A which it says shows she was impersonating its customer and attempting to commit fraud. That's because what I've said above is evidence enough to conclude Santander have fairly loaded the CIFAS marker against Miss P.

That said, and for the sake of completeness, I have listened to both calls. It's possible the call with Bank A and the call I've heard Miss P carry out with our investigator are the same person. They sound *similar*. But I don't need to determine if they're the same person, as there is evidence enough here to conclude Santander acted fairly in loading the CIFAS marker against Miss P without having to make that finding.

My final decision

For the reasons I've explained above, I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss P to accept or reject my decision before 20 July 2021.

Ketan Nagla
Ombudsman