DRN-4326494

The complaint

Mrs W complained because Santander UK plc refused to refund her for transactions on her credit card totalling £2,628.50, which she said she didn't make.

What happened

On 30 April 2022, Mrs W received an email from Santander, saying that 90% of her credit card limit of £3,000 had been used. She couldn't get through to Santander by phone, so went to the branch where she'd opened the account some years before. The transactions which Mrs W didn't recognise were:

- £20.90 at 4:36 am on 23 February to an international money transfer company;
- Four £301.90 payments to the same company at 20:10 pm on 27 March, 8 April (at 16:54 and another at 18:29), and at 23:50 on 13 April;
- Two £300 payments to a cryptocurrency organisation on 20 April (two payments, one at 19:34 and another at 20:26);
- Two £300 payments to the same international money transfer company on 28 April (at 10:59 and 23:16), and one £200 payment to the same company on 29 April (at 21:12).

Mrs W said the branch staff were very helpful and noted that these transactions didn't conform to her usual spending patterns. She normally used her card for food shopping at a number of the larger supermarkets which she used regularly. Mrs W didn't have paper statements, and paid her card by monthly direct debit.

In early May, Mrs W received a letter from Santander, saying it had tried to phone her and asked her to ring back. When she did, Santander told her that the last disputed transactions had been verified by a one-time passcode being sent to her mobile number, which had then been accurately typed into the device making each payment.

Mrs W complained, saying she hadn't received a one-time passcode. She said her phone was a pay-as-you-go phone and wasn't a smart phone, so she questioned how the transactions had been authorised. She also said that the transactions didn't match her usual spending, so Santander shouldn't have let them go through.

Mrs W also contacted her phone provider, and the police, and her husband tried to contact the recipient organisations to try to find out where the disputed money transfers had been sent to. She also got her laptop reviewed by an IT professional who found no malware or viruses which could transmit information without her knowledge.

On 24 June, Santander wrote to Mrs W. It said that as Mrs W had said her phone didn't leave her, and that she hadn't given anyone else one-time-passcodes, there was no evidence that the payments could have been made by any third party. Santander acknowledge that the transactions didn't match Mrs W's usual spending, but said the one-time-passcodes sent to her mobile for all but the smaller initial payment, were a second level of security. And as the one-time-passcodes had been entered correctly, Santander had had no concerns about the payments.

Santander also said that before a one-time-passcode is sent out, its systems checked whether the SIM in a phone had been swapped. This came back confirming there hadn't been a swap. Mrs W's phone provider had told her that this hadn't happened.

Mrs W's phone provider also told her that her phone showed no records either of incoming calls, nor of incoming text messages for one-time-passcodes. It explained that pay-as-you-go phone didn't keep the records of text messages sent and received, but that wasn't the case for incoming phone calls. Santander said that using one-time-passcodes for authentication met with current banking regulations for fraud prevention.

Mrs W didn't accept this. Santander wrote again in late August, but didn't change its decision, because it said it had sent out one-time-passcodes.

Mrs W wasn't satisfied and contacted this service. She said that she hadn't authorised the transactions and hadn't received any one-time-passcodes. She said she didn't believe Santander had done enough to prevent fraudulent activity on her credit card, when the payments didn't match her normal spend. She also said that she didn't have access to online banking apps through her phone, and although Santander said it had tried to contact her several times on her mobile, she hadn't received any calls – which her phone provider had checked and confirmed. She said the transactions hadn't been made from her computer, but Santander still believed she'd made the transactions. Mrs W said she lived with her husband and one of her sons, with her other son visiting and staying overnight occasionally.

Mrs W also said that she'd contacted the two organisations which had received the funds, but they couldn't give her information about the recipients because of data protection. She'd paid the balance off the card so she didn't incur interest, and had a replacement card where she'd reduced the credit limit to protect herself. But as well as the financial loss, she said it had caused her and her family a lot of stress, and had taken up a lot of time through visiting branches, phone calls, emails and sending correspondence.

Mrs W also told our investigator that her phone, which didn't have internet access and wasn't a smartphone, normally lived on a table in her living room, or in an inside coat pocket if she went out. But it wasn't normally switched on – so it would have been difficult for any one-time-passcode to have been verified during the five-minute time limit she'd been told was required by Santander's security system. She said no-one else had access to her phone apart from her husband and sons, but they had their own phones so wouldn't have any use for hers.

Mrs W also said that she and her family had looked up the IP addresses (a unique computer identifier) from where the payments had been sent. She said that they appeared to be in a city centre, a long way from her home address. She said she'd mentioned this to Santander, but it still believed Mrs W had authorised the transactions.

Our investigator didn't uphold Mrs W's complaint. She said that Mrs W's mobile number was the same as the number on Santander's records, to which a one-time-passcode had been sent. The investigator said that based on what Santander, and Mrs W's phone provider, had said, it wasn't likely that the SIM in her phone had been swapped. The investigator said that the transactions were properly authenticated using the one-time-passcode which had been sent to Mrs W's registered mobile number.

Mrs W didn't agree. She said that the investigator had only considered the first seven transactions and not the three on 28 and 29 April. We contacted Santander, which agreed to these being considered, and I've included them in the above information about what happened.

Mrs W also said that:

- most of her normal transactions were for food shopping at local supermarkets. She said she had also made a very small number of transactions to companies for goods to be delivered to her home. But the large transactions to the international payment transfer company, and the cryptocurrency organisation, were so far removed from her normal spend that she couldn't understand why Santander believed she'd authorised them;

- her phone company and Santander had said her SIM within her phone hadn't been swapped, so she accepted that. But she said she'd never received a text message containing a one-time-passcode to her phone. Mrs W said her son had been looking into possible technical answers to why she'd never received the codes on her phone. She sent links to a number of articles which said that third parties could redirect text messages or calls, to another device – a phone or computer which the third party owned. She said that the articles mention that banks are aware of the security issues around the use of text messages as a way of sending verification to authorise transactions. And she said that this would explain why she never received either the one-time passcodes – or any of Santander's subsequent phone calls to her. For example, Santander had said it tried to ring her three times on 26 April to speak to her about the amount of credit left – and even if her phone had been switched off, there'd have been a record of these calls on the phone.

- Mrs W said Santander was basing the whole of its defence on the fact that one-time-passcodes had been sent through text; that they'd reached her; and that she'd submitted them. But if the information in the articles was right, it was possible that both she and Santander had been the victims of fraud.

Mrs W asked for an ombudsman's decision.

My provisional findings

I issued a provisional decision on this complaint. This was because I'd come to a different conclusion to the investigator. Issuing a provisional decision gave both sides the opportunity to comment on it, by the date set, before I issued a final decision

Before issuing the provisional decision, I considered all the available evidence and arguments to decide what would be fair and reasonable in the circumstances of this complaint.

Regulations

In my provisional decision, I explained that in these circumstances there are regulations which govern disputed transactions. The relevant regulations here are the Payment Services Regulations 2017. In general terms, the bank is liable if the customer didn't authorise the payments, and the customer is liable if they did authorise them.

So I carefully considered who I thought was most likely to have authorised the disputed payments.

Is Mrs W likely to have authorised the payments herself?

I could see from Mrs W's statements that it was clear that the disputed transactions were indeed very different in nature from Mrs W's normal spend. Her credit card statements showed a pattern of supermarket spend and very occasional other small transactions, which

looked like payment for goods to be delivered to her home, as she said. I saw no other transactions to international money transfer organisations, or cryptocurrency organisations.

I also considered Mrs W's circumstances. These included her mobile being with her at home, turned off, during the day unless she's going out. Mrs W didn't use any banking apps and only authorised small internet payments infrequently using her computer, for specific small purchases. This isn't a typical profile for anyone who is likely to be comfortable making large internet payments either to international money transfer organisations or to cryptocurrency organisations.

I also bore in mind the time of day when the disputed transactions took place. The first one took place at 4.36am and was a small payment for £20.90. I think it's most likely that this was a test by whoever made the transactions, to see whether it would be spotted before making a further payment. The larger payments took place after Mrs W – who didn't have paper statements to check – didn't immediately raise the alarm. The later transactions then took place in the late afternoon or evening, and in one instance just before midnight. As Mrs W appears to have been generally at home during the daytimes, I thought that if she'd authorised the payments herself, she'd have done so during the day, not at these times.

Santander provided us with the IP addresses (a unique computer identifier) for the disputed transactions. There was a range of IP addresses, most of which were in a large city several hundred miles away from the rural area where Mrs W lives. There were some recorded log-ins, on 22 February and 3 March, which used an IP address which had been used to log into Mrs W's online banking before. There are no payments on those dates, so it's possible that someone else was trying to log on to check access. IP addresses can be disguised or hidden, but it's also possible that whoever carried out the transactions was away for work, or was being assisted by someone else.

Mrs W had also been very active in pursuing her claim. She'd gone to a lot of trouble: visiting her phone provider many times; going to her Santander branch many times; researching IP addresses and how secure one-time-passcodes are; trying to contact the firms which received the money from her account; as well as contacting the police and Action Fraud. She also got her laptop checked by an IT professional for any malware or viruses, which would have incurred a cost. It's not impossible that someone who had actually authorised the transactions themselves might do some of this to make their claim appear genuine. But I thought that going to all this trouble persuaded me that Mrs W was more likely than not unaware of the transactions she's disputing, and didn't consent to them in any way.

So for all these reasons I thought it was unlikely that Mrs W authorised the disputed transactions herself.

Who else might have authorised the payments?

Mrs W said she hadn't had her phone or card lost or stolen. She hadn't received any cold calls, emails or texts, or divulged her card details to anyone. But the transactions did take place, so someone must have obtained her details.

Mrs W provided links to online information, which she said one of her sons researched for her, which said that a one-time-passcode security system can easily be got round. These said that third parties can redirect text messages or calls, to another device – a phone or computer which the third party owned. Some of the website information provided by Mrs W is very general, and I wasn't persuaded that something so unusual was the answer here. It was much more likely that whoever carried out the transactions had access to Mrs W's phone, received the one-time passcodes, then deleted them from the phone.

The key issue was that whoever carried out the transactions must have had regular access, over several months, to Mrs W's card, Santander account details, and phone. Mrs W's credit limit was £3,000, and the disputed transactions come to just over £2,600. Mrs W had some genuine spending too, so it's likely that whoever carried out the transactions knew what Mrs W's credit limit was, and stuck below that limit to avoid the transactions being stopped by Santander.

So I asked for more information from the recipient organisations. One didn't reply, but we heard back from the international money transfer organisation to which eight of the ten disputed transactions had been sent. I asked it to tell us about the account to which Mrs W's money had gone, and it sent us information about the name of the individual to whose account the credits went. For data protection, we aren't allowed to provide Mrs W with the name of that person. But we could tell her that it was someone with the same surname as her, and the first name tallied with one of the names she'd mentioned as being part of her household.

In the provisional decision, I recognised this was a very difficult message. But it also explained many of the features of these transactions. Someone who had access to Mrs W's home was in the best position to obtain her card details, and her phone. For example, it would explain the odd times of day when they took place.

We gave Mrs W the limited information we could pass on and asked for her comments. Mrs W was understandably interested in exploring any other possibilities, instead of the conclusion to which the new information led. She suggested that Santander might have disclosed her information to a fraudster; she asked if we could force a reply from the cryptocurrency organisation to which the other two of the ten payments went; or thought someone unknown to her might have used the dark web to obtain her personal data to make the transactions.

We exchanged several emails, but my view remained that it was most likely that someone known to Mrs W, with access to her home and her phone and security details, carried out all ten transactions. I explained that it wasn't my view that Santander had either carried out the disputed transactions itself, or disclosed her details to a third party. Clearly it would have been helpful to have a reply from the cryptocurrency organisation which received two payments, as well as the international payment organisation which received eight payments. But neither the cryptocurrency organisation nor the international payment organisation had been under any obligation to respond, and we were fortunate that the latter chose to be helpful. But it was unlikely that different individuals would have been able to take money out of Mrs W's account, because the use of her phone, security details, and timing of the payments indicated it was someone with access to her home. So I considered it was likely that all ten payments were carried out by, and benefitted, the same person.

I didn't think it likely that the dark web had been involved, as the evidence didn't point to this being likely. And if a third party fraudster had obtained her details, it wasn't at all likely that they'd have credited an account in the name of a person with the same name as one of Mrs W's other three household members. Whoever opened the account would also have had to provide identity in that name.

Transactions carried out by a household member without the account holder's consent – what the Regulations say

As I set out above, a customer is liable if they've authorised the transactions, and I accepted on the evidence that Mrs W didn't authorise them. I thought it was most likely that they were carried out by a member of her family with access to her card and phone, so I looked at the Regulations about this situation.

These transactions were carried out on a credit card, and slightly different rules apply from transactions on a debit card. On a debit card, the account holder can be liable if they've not kept their devices and details secure, as it can under certain circumstances count as ''*gross negligence''*. But that doesn't apply on a credit card. And in any event, Mrs W wouldn't have expected to need to hide her phone and security information from a family member whom she trusted.

As I had concluded that Mrs W was unaware of the disputed transactions and didn't authorise them herself, I found that she wasn't liable for the disputed transactions under the Regulations, so Santander should refund her. Nor could I see any other reason why it would be fair and reasonable for Santander to hold Mrs W liable for the transactions here. But, for completeness, I also considered whether Santander should have blocked the transactions as they were attempted.

Should Santander have blocked the transactions?

Banks have an obligation to process the payments its customers authorise it to make. There's a balance between intervening to prevent fraud, and the risk of unnecessarily inconveniencing or delaying legitimate transactions. I would expect a bank's systems to take into account whether transactions were out of character and unusual. This uses a range of features, and as a security issue the exact algorithm wouldn't be made public. But I'd expect it to include, for instance, whether the amount of the payments was out of character and unusual.

The disputed transactions were out of character for Mrs W's account, both in size and amount, but also in terms of going to an international money transfer organisation and to a cryptocurrency organisation. Santander sent one-time passcode for all but the smallest of the transactions, but that wouldn't be any protection if, as I considered likely, they were carried out by someone with access to Mrs W's device. The one-time passcodes would have been received by, and the payments confirmed by, that person.

So I considered that although the first, £20.90 payment, was small and might not have been stopped, I think Santander could have blocked the remaining nine payments in any case. In practice, however, this makes little difference because Mrs W didn't authorise the payments, so under the Regulations, Santander has to refund Mrs W for all ten unauthorised payments.

So my provisional decision was that I intended to uphold this complaint, and to order Santander UK plc to pay Mrs W:

- £2,628.50, representing her financial loss for the ten disputed transactions which she didn't authorise; and
- Interest at 8% simple on this amount, from the dates of each of the ten disputed transactions to the date of payment; and
- If Santander deducts tax from the interest on the award, it should provide Mrs W with a tax deduction certificate to show how much it has deducted, in order to allow Mrs W to reclaim the tax from HMRC if appropriate to her personal circumstances.

Responses to my provisional decision

Mrs W didn't reply to the provisional decision by the date set.

Santander asked for some more information from Mrs W. It asked for the crime reference number from when Mrs W first contacted the police. It also asked, in order to reduce future

risk, what security precautions Mrs W is now taking with her credit card and mobile phone to prevent this happening in future.

Mrs W answered Santander's questions, and we passed her reply on to Santander. Santander didn't comment further by the date set.

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 reconsidered, I find that my original conclusions were fair and reasonable in all the circumstances of this complaint.

It's clear from the circumstances of this sad case, and Mrs W's responses, that the theft which took place has had a significant impact on Mrs W, and has changed the way she and her family live. I'm sorry that this has been so distressing, and I suggest that she might find it helpful to contact Victim Support.

My final decision

My final decision is that I uphold this complaint. I order Santander UK plc to pay Mrs W:

- £2,628.50, representing her financial loss for the ten disputed transactions which she didn't authorise; and
- Interest at 8% simple on this amount, from the dates of each of the ten disputed transactions to the date of payment; and
- If Santander deducts tax from the interest on the award, it should provide Mrs W with a tax deduction certificate to show how much it has deducted, in order to allow Mrs W to reclaim the tax from HMRC if appropriate to her personal circumstances.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs W to accept or reject my decision before 28 September 2023.

Belinda Knight
Ombudsman