DRN-4309366

The complaint

Mrs M is unhappy that Santander UK Plc hasn't refunded transactions made using her debit card which she says she didn't authorise.

What happened

Mrs M says she woke up on the morning of 12 March 2023 to find a text message from Santander on her phone. The message said that Mrs M's account was overdrawn. She thought that couldn't be right as she'd not made any recent payments from her account.

Mrs M logged onto her online banking and could see two transactions she didn't recognise, for the purchase of gift vouchers online, through an overseas merchant. She froze her card and contacted Santander to say she'd been the victim of fraud. While on the phone, the Santander representative said he could see further attempts to use the card.

Santander went on to consider whether it would refund Mrs M. But once it had investigated it said it wouldn't do so as it wasn't persuaded the transactions were unauthorised. Santander's main reason for reaching that position was because it could see the transactions had been made using a device (since identified as Mrs M's husband's laptop) that had previously been used for genuine, undisputed transactions.

Mrs M didn't agree with Santander's position and so brought the complaint to our service. One of our investigators considered the complaint but didn't uphold it. He felt Santander had acted fairly and reasonably in declining to refund Mrs M. In summary, he said:

- the device was confirmed as one genuinely used by Mrs M;
- that same device had previously been used to transact against Mrs M's account with the same IP address that Mrs M most often used;
- there was no explanation as to how an unknown third-party might have gained access to the card details, including the CVV security number (which was required and input for the disputed transactions).

He then concluded it had been fair and reasonable for Santander to say the transactions were authorised and that Mrs M would be responsible for them.

Mrs M disagreed with that outcome and asked that an ombudsman review her complaint. She also asked for a copy of the evidence relied upon, which has since been provided. The complaint has now been passed to me for a final 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.

I'm sorry to disappoint Mrs M further but I'm not upholding her complaint. I know from what Mrs M has said before that she feels very strongly about her case, which is understandable.

I know it will also be disappointing that I'm unable to tell Mrs M exactly what has happened here. But it isn't my role to do so. My role is to consider all the available evidence and information and decide whether Santander has acted fairly and reasonably in the

circumstances. In practice, that means making my decision on the balance of probabilities – that is to say what I consider is more likely than not to have happened.

The relevant test for considering Mrs M's complaint arises from the Payment Service Regulations (2017). Broadly speaking, these set out that a customer will be responsible for any transactions out of their account that have been properly authorised.

In order to demonstrate proper authorisation, and so hold a customer responsible for transactions which debit the account, the bank must evidence two things: that the transaction(s) was properly authenticated and that the customer gave their consent for it.

Authentication

For the authentication of online transactions, like the ones in dispute here, I'd expect the bank to be able to show that the correct card details were entered and that the CVV was supplied. That evidence has been given and is quite unequivocal. The evidence also shows that there was a 3DS check – an additional layer of security – carried out before the payments were allowed to go through.

I'm satisfied Santander has shown sufficient and persuasive evidence that the transactions were properly authenticated. This isn't surprising as, without proper authentication, it's unlikely the transactions would have debited Mrs M's account, let alone her being held responsible for them.

Consent

The question of consent is where a greater degree of investigation is required. Santander can't rely solely on the entering of the card details to establish consent. It's here where different scenarios to explain what might have happened ought to be considered.

It is the case that card details might be compromised in any number of ways. It will often be the case that the customer – like Mrs M – may have no idea how those details became compromised. That fact wouldn't mean that a fraud claim is automatically not upheld. The wider circumstances must be considered.

I've looked at the evidence on file and I'm satisfied that the device used to make the transactions was one that had been legitimately used by Mrs M in the past. Mrs M's own testimony confirms that to be the case.

She's confirmed a genuine transaction made using that device. I can see that device has previously been linked with the same IP address as Mrs M frequently uses to log onto online banking. I consider these two points to be very persuasive in showing that the transactions were conducted on what has been identified as Mrs M's husband's laptop.

Mrs M has suggested that a fraudster could have somehow cloned the device ID that was recorded by the bank, or otherwise tricked it into believing the transactions were being made from an existing device. I'm not persuaded that is the more likely than not explanation.

There is the question as to why a fraudster would go to such lengths. If they were in possession of all the details required to make a transaction, there would be little benefit in them trying to clone a device ID. Arguably it might mean a transaction was less likely to be picked up by the bank's account monitoring. But the payments were relatively low in value here, so it seems there was little risk of that in any case.

I know Mrs M has found some information about device cloning online. But there's little to suggest that's what has happened, given this would be an isolated (no other attempts against Mrs M's or the household's other accounts) and limited (in terms of value) attack.

That being the case, there doesn't then appear to be a reasonable explanation for how an unknown party could have gained access to the laptop to make the transaction. I know Mrs M has said only her and her husband were in the house at the time, and that the laptop was turned off. But the evidence I have very strongly suggests that wasn't the case.

I've thought about what else the evidence shows, and I've used that to help inform my findings. Of note is the timing/pattern of transactions. The first disputed transaction takes place at 18:06 on 11 March 2023. The second is at 06:54 on 12 March 2023. So there are nearly thirteen hours between the two disputed transactions. I'd expect an unknown fraudster to act more quickly to try and maximise the amount obtained. To delay is to increase the risk of being discovered. Here, the gap between the transactions is large, especially when considered in the context of a fraudster being in operation. The further attempts to execute more transactions are another hour later, for further context.

The payments aren't made in the middle of the night, when they might go unnoticed; they are at times when most people would be awake. I'm then led to find that such a fraudster being in operation isn't the more likely than not scenario here.

I can accept, in making that finding, that it's possible a fraudster might delay payments to try and avoid triggering a bank's security. But I'd refer to the points I've already made in that regard.

I have also thought about the failed transactions, one of which even seems to be attempted whilst Mrs M is talking to the bank. Those failed payments would seem to support Mrs M's version of events: that she didn't make or otherwise authorise any of the account activity. But I don't find those failed transactions represent strong enough reason to overturn the other evidence available.

There is further evidence the failed transactions can provide. The final one attempted was for £90 to a UK based garden centre. Mrs M has said that this was also an unauthorised attempt.

The evidence available for this transaction shows that a CVV was not entered when the payment was attempted. That would normally suggest that the merchant has been used previously, and has a record of the CVV, meaning a check against it and the triggering of the 3DS system wouldn't be required. That being the case, the evidence points to it being a transaction genuinely attempted. That is the on balance finding I'm led to.

Mrs M has questioned some of the evidence, particularly around IP addresses and device IDs. I acknowledge that some of the evidence comes across as confusing and unclear, perhaps even contradictory at times. I can assure her that I have carefully reviewed the technical evidence and am satisfied by what it shows in terms of device IDs and IP addresses. I'm afraid I can't give her a more detailed breakdown of the evidence here.

One of the IP addresses Mrs M has raised particular concern about is one that seems to be based in the US. She's pointed out that the fact it is first recorded against her banking on 12 March 2023 – just when the disputed transactions are occurring – is suspicious and helps to indicate fraud is taking place. I can understand her concern here, but I can explain two important points about the IP address:

- It is first recorded at 7:19 on 12 March 2023, which is after the two disputed transactions had been made. It is therefore unconnected to them.
- The supporting evidence shows the activity connected to the IP address is the freezing of Mrs M's card. That is the one and only activity linked to it. I can also see another US based IP address being registered on 18 March 2023. The evidence shows the connected activity was Mrs M viewing her PIN. It then becomes apparent that these US based IP addresses are generated when activity related to card security is taking place. I can't tell Mrs M why that is the case, but I'm satisfied it is, and that there isn't an underlying indication of fraud or something suspicious happening.

With these points in mind, I'm satisfied the US based IP addresses aren't connected to the disputed transactions, and they don't alter my findings.

I can't be certain of what has happened here; I can't tell Mrs M exactly how the transactions came to debit her account. But, having considered all the evidence, I can't see there's a persuasive explanation as to how an unknown fraudster could have carried out the disputed transactions. It then follows that I must conclude they were authorised, and that Santander has acted fairly and reasonably in not refunding Mrs M.

Should Santander have intervened?

Given my findings on authorisation, any consideration about Santander questioning the payments at the time they were being made must fall away. But, even so, the two that successfully debited Mrs M's account weren't so unusual in nature (considering their value, timing, and Mrs M's normal account activity) that I'd find Santander ought to have stepped in to question them in any case.

My final decision

I don't uphold this complaint against Santander UK Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs M to accept or reject my decision before 10 February 2024.

Ben Murray
Ombudsman