DRN-4594534

The complaint

Mrs O has complained that State Bank of India (UK) Limited ("SBI") won't refund transactions she says she didn't make or otherwise authorise.

What happened

In April 2020, Mrs O's registered mobile phone number was changed. This was verified by a security call. In May 2020, the new mobile was used to reset her password, then send out around £6,000 over several bank transfers, verified by one-time passcodes sent to Mrs O's email address. SBI sent Mrs O notifications about the activity by email and letter.

In June 2023, Mrs O reported the transactions as fraudulent. She said she hadn't been receiving her statements, and the new mobile phone number wasn't hers. She hadn't lost her card, hadn't recorded or shared her security details, and hadn't been pressured into making the payments.

SBI held Mrs O liable for the payments in dispute, as her security details and email address had been used, and they'd sent her notifications about the activity at the time, as well as her annual statements.

Our investigator looked into things independently and didn't uphold the complaint. Mrs O's representatives didn't agree, so the complaint's been passed to me to decide.

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.

In doing so, I have taken into account everything which both sides have said and provided. But I won't comment on absolutely everything – we're an informal alternative to the courts and don't necessarily address things on a point-by-point basis. Instead, I've focused my decision on what I've found to be the key points.

I should also explain that in this dispute between Mrs O and SBI, I am only considering whether SBI can hold Mrs O liable for the disputed payments or not. I am not a police force and cannot carry out a criminal investigation into who exactly may have made the payments.

Broadly speaking, SBI can hold Mrs O liable for the payments in dispute if the evidence suggests that she authorised them.

Because of all the time that's passed, the evidence is more limited than it would've been had Mrs O reported this back in 2020. For example, there's no longer a recording of the call where Mrs O's phone number was changed, as it was too long ago. But according to the electronic records, the security check was completed successfully. That means the person who called was able to provide Mrs O's telephone banking PIN, and answer the security questions to be identified as Mrs O.

It's not clear how someone would know Mrs O's security details without her permission. She said she didn't record them or share them. She wasn't threatened or scammed into giving up access to her account. And I've not found any evidence that her account's security was bypassed.

The password reset and disputed payments were then authenticated using Mrs O's customer ID, and one-time passcodes sent to Mrs O's email address. This was the same email address which Mrs O provided when she opened the account in 2014 – it was not changed in 2020. Again, it's unclear how someone had access to Mrs O's customer ID and email without her permission.

While this is a more minor point, I might generally expect a thief to try to take money as quickly as possible, before the customer realises what's happened and blocks the account. But here, the disputed activity was carried out over the course of 10 days, with a notable delay between the new mobile phone gaining access the account and any money actually being spent.

SBI sent Mrs O notifications about the phone number change and the transactions, by email and letter. According to their electronic records, they also sent her regular statements to the address on file, which is the same address Mrs O gave us. So it's most likely that Mrs O was made reasonably aware of the activity at the time. But she didn't tell SBI anything was wrong for over three years. It seems unlikely that Mrs O would wait so long to report the disputed payments if they were made without her consent.

Mrs O's representatives suggested that an SBI staff member may have compromised her security details, either fraudulently or by accident. But staff members don't have access to customers' security details. I've found no evidence which shows or substantiates that this was a staff member's fault.

In summary, the person making the disputed payments had Mrs O's telephone banking PIN, customer ID, full access to her email, and sufficient knowledge of her security details that they could be identified as Mrs O over the phone. The person using the account did so relatively slowly, seemingly confident that Mrs O would not block them. And Mrs O was made reasonably aware of the activity, but didn't report anything being wrong for several years. So based on the evidence, there doesn't seem to be a likely way that the disputed payments could've been made without Mrs O's consent. Whereas it does seem both likely and plausible that these payments could've been made by Mrs O or by someone she gave her permission to.

On that basis, it seems fair that SBI declined a refund in this case. I do appreciate that this is not the outcome Mrs O was hoping for. But given the evidence I have, and the balance of probabilities, I'm unable to reasonably reach any other conclusion.

My final decision

For the reasons I've explained, I don't uphold Mrs O's complaint in this case.

This final decision marks the end of our service's consideration of the complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs O to accept or reject my decision before 17 April 2024.

Adam Charles
Ombudsman