DRN-4395294

The complaint

Mr D has complained that TSB Bank plc won't refund transactions he says he didn't make or otherwise authorise.

What happened

Over the course of several days, Mr D's TSB mobile app was used to send around £2,900 worth of bank transfers.

Mr D says this wasn't him. He explained his phone was stolen on a night out. He didn't keep a record of his security details or share them with anyone. Mr D thought the thief might've watched him enter his phone's passcode before stealing the phone, and he said he'd set his online banking password to be the same as the phone's passcode. He had not received any suspicious communications, clicked any suspicious links, or downloaded any new apps recently.

TSB held Mr D liable for the payments in dispute. He came to our service.

Our investigator looked into things independently and didn't uphold the complaint. They found that the payments had also used Mr D's secondary security details, not just his password, and they didn't see a likely way someone had learned that without his consent. And they'd been made from Mr D's usual IP addresses.

Mr D appealed, 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.

Broadly speaking, TSB can hold Mr D liable for the payments in dispute if the evidence suggests that he authorised them.

I'm satisfied from TSB's technical evidence that the payments in dispute were made on Mr D's genuine mobile app, on his registered device, using his login details and security details. I can see that these transactions were properly authenticated. The question, then, is whether the evidence suggests that it's most likely Mr D consented to the payments or not.

It's possible that a thief could've watched Mr D enter his phone's passcode, then apparently used the same passcode to log in to his TSB app. However, the payments also used Mr D's secondary security details, which were different to his passcode. And Mr D was clear that he didn't tell anyone his security details nor record them anywhere. There's no evidence of any unauthorised access, hacking, or security being bypassed, and from what Mr D told us there doesn't seem to be a likely way he could've been hacked. As I said above, I'm satisfied that these payments were properly authenticated.

On that basis, there's not a likely or plausible way that someone had Mr D's secondary security details without his consent. That would mean these payments were most likely authorised, and so TSB do not need to refund them. This possibility is also supported by the fact that the disputed payments were made from IP addresses which Mr D also used for his genuine online banking activity before and after, suggesting that the person who made the payments was accessing Mr D's phone from the same locations he normally used it in. It also looks like Mr D used the same mobile phone for genuine online activity after it was supposed to have been stolen.

I appreciate why Mr D would like to see CCTV footage. Such footage is only kept for about a month as standard, so it'll be too late for that. But it's also not really relevant here. These payments were made online, not at a physical cash machine or shop. And camera footage would only show what the person making the transactions looked like. It would not have shown whether they had Mr D's permission or not. And as I explained above, based on the evidence it's not likely or plausible that the payments were made without Mr D's consent.

I also appreciate that Mr D would have liked TSB to stop these payments at the time. As they were made on Mr D's device, at his usual IP addresses, using his correct login details and security details, it would've looked like it was Mr D making the payments himself. I don't see that TSB needed to stop them at the time.

Lastly, Mr D complained about TSB's customer service and them blocking his account. It was correct for TSB to block the account when he reported the fraud, as Mr D had told them that a fraudster had full access to it, so TSB needed to block and secure the account. I can see it was blocked for a week, which was not unreasonable here. And having looked at Mr D's contact with TSB and listened to relevant calls, I've not found that they mishandled things overall or dealt with him inappropriately.

In summary, I'm satisfied that Mr D's genuine phone, app, login details, and security details were used. Based on the evidence, it's not likely or plausible that the payments could've been made without Mr D's consent. That means TSB can decline a refund in this case. This is a difficult message for me to give, and I know it's a difficult message for Mr D to receive. 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 Mr D's complaint.

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

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr D to accept or reject my decision before 28 November 2023.

Adam Charles
Ombudsman