DRN-5798543

The complaint

Mr E complains that TSB Bank plc ("TSB") failed to refund transactions he didn't recognise.

What happened

Mr E noticed his account had less money than it should've after trying to purchase an item. He reported this to TSB, where it became apparent that a number of bank transfers (faster payments) had been made from his account that amounted to more than £1,000. Payments had gone to two different accounts after Mr E's mobile banking had been re-activated.

Mr E said he wasn't using his mobile banking at the time and wasn't aware of these transactions. He said he'd had some difficulties with payments and his debit card had recently been replaced. Mr E believed that unknown third parties were responsible for the payments from his account.

TSB looked into what had happened and advised Mr E that a new device had been registered the day of the bank transfers. This had required a password re-set and part of that process was to send a One Time Passcode (OTP) to Mr E's phone. TSB confirmed that the only number they had for Mr E was the one he provided to them, which is the same one given to our service.

TSB only had one email address recorded for Mr E. Together with the necessary security information for Mr E's account, the newly registered device set up the new payments and proceeded to send money to two different banks (the accounts later turned out to be credit card company accounts).

TSB declined to refund Mr E as they couldn't see how the various details required to set up and use Mr E's mobile banking could have been acquired without his knowledge. Mr E denied receiving any information or passing his details to anyone else. After complaining, TSB again declined to refund him.

Unhappy with their outcome, Mr E brought his complaint to the Financial Ombudsman Service for an independent review. An investigator was assigned to look into the matter and both parties were asked to provide information about what had happened.

Mr E confirmed his version of events and reiterated that no one else had access to his information or his phone. He continued to argue that others were responsible. Mr E confirmed he hadn't been asked by anyone else to pass them his details. He also confirmed he was a regular computer user but hadn't clicked on any unusual links. Mr E also said he hadn't seen any OTP on his phone.

TSB provided details of the payments and the audit logs concerning the use of Mr E's mobile banking application. This showed a new device was registered on the day of the disputed transactions. They also provided details of the OTP and confirmed the information they held for Mr E, including his phone and email address.

After reviewing the evidence, the investigator didn't think TSB had acted unfairly and thought

it was more likely than not that Mr E was responsible for the payments himself. It was commented that there was no evidence to support a compromise of his banking information. The OTP was sent his phone, without which the new device couldn't have been registered.

Further information from the recipient banks was received, confirming the accounts that received the funds weren't in Mr E's name.

As no agreement could be reached, the complaint has now been passed to me for a 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.

The relevant law surrounding authorisations are the Payment Service Regulations 2017 (PSRs). The basic position is that TSB can hold Mr E liable for the disputed payments if the evidence suggests that it's more likely than not that he made them or authorised them, but TSB cannot say that the use of the internet banking facility to send faster payments conclusively proves that the payments were authorised.

Unless TSB can show that consent has been given, it has no authority to make the payment or to debit Mr E's account and any such transaction must be regarded as unauthorised. To start with, I've seen the bank's technical evidence for the disputed transactions. It shows that the transactions were authenticated using the payment tools issued to Mr E.

It's not my role to say exactly what happened, but to decide whether TSB can reasonably hold Mr E liable for these transactions or not. In doing so, I'll be considering what is most likely on a balance of probabilities.

When the faster payments were made, they used a newly registered device (likely a mobile phone) to set up and send them to two different accounts – both related to credit card accounts not in Mr E's name. If this was fraud, the payments to an individual's credit account are not a typical destination for such payments as they're easily tracked. Someone stealing Mr E's funds who had full access to his account (as is the case here) could easily send the money to other destinations that would make recovering or identifying the user much more difficult.

The registration of the device required several different pieces of information which Mr E has said were only known to himself. He denies giving them to anyone else and said he hasn't clicked on any suspicious links. So, for the purposes of this complaint, I've taken Mr E's position to be that he wasn't asked or coerced into making payments by anyone else. If this was the case, both the bank and our service would address the issue differently – as a scam.

As Mr E has said he wasn't scammed, I've gone on to consider the likelihood that somehow his security information for his account and access to his phone were obtained by an unknown third party without his permission. TSB's records show a consistent phone number given to them by Mr E which they used to send the OTP. This was an important step in the registration of the new device. That OTP had to be used by whoever registered the new phone.

Additionally here, there were other details about the account known only to Mr E that would've been needed to set up the new device. Looking at the online records, Mr E hadn't used the online banking for some time (the last use was the previous year), so it's

reasonable to conclude he wasn't a regular user of the account.

I noted that there was a password re-set that started the process (which wouldn't be so unusual after not using the account for such a long time) and according to TSB's own instructions, this would've needed access to Mr E's memorable information. This was required to be entered into the mobile banking app before the re-set could've been successful.

Given that Mr E has stated he hadn't given this information to anyone else, it's difficult to see how this could've been known to an unknown third party acting without his knowledge or instruction.

So, based on the requirement to have access to Mr E's mobile phone, obtain his memorable information, have knowledge of his account and personal details and the type of payments made to identifiable credit accounts, I think it unlikely this could've been carried out by an unknown third party.

I have thought about whether Mr E was somehow persuaded to give access to someone else in order to allow his account to be used to make one or some of these payments (not in the context of a scam – but rather allowing someone else to use the account). If this was the case, I would likely conclude that he'd intentionally provided access to his account, so it wouldn't be fair or reasonable for TSB to make a refund. I'm not making a specific finding about this here because Mr E's position is that he wasn't persuaded to hand over anything. I have referred to it based on the overall evidence and the lack of a plausible explanation for how these transactions took place.

Based on Mr E's argument, I haven't been able to find evidence that supports his position. I think it's implausible to conclude they weren't authorised without stronger evidence to the contrary. That means I think it's more likely than not that Mr E was responsible for the registration of the new device and the disputed payments made from his account – or that someone else with consent did so.

My final decision

My final decision is that I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr E to accept or reject my decision before 6 October 2025.

David Perry
Ombudsman