

## **The complaint**

Mr G complains TSB Bank plc (“TSB”) refuses to refund him for unauthorised transactions on his account.

## **What happened**

The facts of this case are well known to both parties, so I won’t repeat them in detail here.

In short, Mr G says he was contacted on 25 September 2023 by someone he thought was TSB informing him that his account and online banking was blocked for fraud prevention. However, after regaining access to his account and online banking on 1 October 2023 he noticed unauthorised transactions on his account. He says TSB should refund these as unauthorised, and it should have blocked them in the first place.

TSB says the transactions in dispute were carried out on a new device added to his account on 25 September 2023. It has no record of it calling him on that date. It says there is also evidence of a password and memorable information change on his account, all which was completed after confirming the one-time passcode (OTP) sent to Mr G’s registered mobile phone number. And as Mr G says he hasn’t given this to anyone else, he must have made these changes himself and therefore made the transactions himself. It also says its fraud team did flag some of the payments as suspicious and sent him SMS messages about these. However, the transactions were processed after it received a call from who it believes was Mr G confirming them as genuine.

Our investigator considered this complaint in full and decided not to uphold it. With the evidence supplied by Mr G she was not persuaded the transactions were unauthorised and felt there wasn’t anything else she could’ve reasonably expected TSB to do in the circumstances. Mr G didn’t agree with this outcome, so the complaint has 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.

Before I set out my thoughts, I want to acknowledge that I have summarised this complaint briefly and, in less detail, than has been provided. I’ve focused on what I think is the heart of the matter. Please rest assured that while I may not comment on every point raised, I have considered it. I’m satisfied that I don’t need to comment on every individual point or argument to be able to reach what I think is the right outcome. Our rules allow me to do this and reflect the fact that we are an informal service and a free alternative for consumers to the courts.

Generally speaking, TSB is required to refund any unauthorised payments made from Mr G’s account. Those rules are set out in the Payment Service Regulations 2017. However, the regulations also say that account holders can still be liable for unauthorised payments under certain circumstances – for example if they’ve failed to keep their details secure to

such an extent that it can be termed "gross negligence." So, I've considered whether it's more likely than not that Mr G authorised the transactions himself, or whether he failed to keep his details secure through gross negligence.

Mr G is adamant that he didn't authorise the transactions in dispute. He is also adamant that he didn't share any OTPs sent to him. However, as I've outlined below, the evidence suggests that both cannot be true. TSB, and our investigator, didn't uphold this complaint and from what I've seen I don't think this outcome is unreasonable. I have also not upheld this complaint and I'll explain why.

TSB has provided evidence to show the transactions in dispute were all completed via a new device, set up on 25 September 2023. It also shows that an OTP was sent to Mr G's registered device to complete this set up. At the same time a password change was completed and a change to the memorable word. Again, TSB has evidenced that this was only completed after the correct OTP was entered. I've seen evidence that Mr G had received OTPs and other messages from TSB from around the time of the disputed transactions. So, I think it's likely he received all the OTP messages sent by TSB.

Mr G is adamant he didn't share the OTP with anyone, even though he says he received a call from who he thought was TSB around the time. His representative says he may have accidentally shared one OTP, but there is no way he could've shared multiple. We have asked many times, but Mr G's position remains the same. From our experience there has been no recorded cases overriding the OTP process. Mr G's representative suggested the possibility that Mr G's phone was compromised. And I agree that is possible, but I haven't seen any evidence which suggests to me this was the most likely possibility. So, on I think it likely Mr G completed these transactions himself or gave the OTPs to someone else to completed them for him.

I've seen evidence that Mr G received multiple messages from TSB throughout the period of disputed transactions. These SMS messages made it clear that transactions were being made on the account which raised suspicions. From the evidence I have Mr G received these messages on 27, 28, 29 September and 1 October. The messages received on the 25 September 2023 include OTPs and clearly say *"Don't share this OTP with anyone – not even TSB."*

There are three possible options here. One is that Mr G carried out the transactions himself. Another option is that he consented to the transactions by allowing someone else to add their device to the account and make these transactions. The third option is that a third-party, unknown to Mr G set up another device on his account using the OTPs Mr G gave them over the phone.

In practical terms, it doesn't make any difference which of these three options happened here. That's because Mr G is liable whether he carried them out himself; or allowed someone else to do so; or was grossly negligent by providing multiple OTPs and ignoring the warnings he received.

Mr G's representative says Mr G suffers from vulnerabilities which should've been considered by TSB. But there is no evidence that Mr G made TSB aware of these difficulties so it would be unfair of me to expect it to have done anything different to help Mr G without that knowledge.

Mr G also says TSB's fraud prevention team should've realised the changes to his account looked suspicious, coupled with several transactions leaving his account. However, from what I've seen TSB did make several attempts to get in contact with Mr G via SMS to question the payments being made. I've listened to the calls it received, and I cannot make a

conclusive finding on whether the caller is Mr G or not. But in any case, I don't think I need to. I say this because I am considering what I expected TSB to do in the circumstances. TSB asked several security questions which were answered correctly and even required the caller to click on a link sent to Mr G's email. All were completed correctly, so think it's fair to say that TSB made reasonable efforts to minimise the risk of fraud occurring here. And overall, I don't think it would be fair for me to suggest it could've done much more.

I appreciate this decision will be very upsetting for Mr G. However, my role is to look at all the evidence, and then reach a decision that takes this into account and is fair to both parties. That means I consider TSB's position as much as I do Mr G's. And what Mr G's asking for here is for TSB to use its own funds to pay him back money that he says was spent from his account fraudulently. But for all the reasons outlined above, I don't think that would be fair.

### **My final decision**

I am not upholding this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr G to accept or reject my decision before 10 March 2025.

Sienna Mahboobani  
**Ombudsman**