

The complaint

Mr B has complained that TSB Bank PLC (“TSB”) sent him an unencrypted email that contained sensitive personal information.

What happened

Mr B had difficulties using the cheque payment feature on TSB’s app. As a result, Mr B submitted a complaint online. When he did that, TSB sent him an email that included an attachment that contained the personal information he’d entered in the online form.

Mr B complained to TSB about this. TSB issued its response on 24 June 2025 and didn’t uphold the complaint.

After Mr B referred his complaint to this service, our investigators assessed the complaint, and they ultimately upheld the complaint and recommended that TSB pay Mr B £30 to cover the cost of a protective registration.

As a resolution to the complaint could not be agreed upon, the matter was referred for an ombudsman’s 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.

Having reviewed everything, I uphold the complaint. I will explain why.

Mr B has complained that, when he filled out an online form, TSB sent him an unencrypted email that contained an attachment containing personal data – such as his name, address, date of birth, contact details, as well as his account number and sort code.

In response, TSB said that its online form says that once the form is complete, a copy of the completed form would be sent to the person who filled it out. Mr B says it doesn’t say this. But when I attempted to fill in the same online complaint form for TSB on its website, to see what was said, under the link you need to click on to open the online complaint form, it says:

“You will receive a copy of the completed form by email”

Nonetheless, I understand that Mr B’s concern is not the fact he received an email as such, but because he says it was sent unencrypted and contained a substantial amount of his personal data within an attachment.

In its response to the investigator’s most recent assessment, TSB says that it has no evidence that it sent Mr B an unsecured email. But from the evidence I have been provided with, it does seem that, although the online form that Mr B completed may’ve been processed using secure processes, the email containing the attachment (which contained Mr B’s personal data) does look to be an unencrypted email. So based on what I have seen, it does look like TSB did send Mr B an unsecured email that included an attachment that contained his personal data.

Given the ever-increasing amount of scams and fraud, I can understand why Mr B may be concerned about this. But I’m also mindful that there is no indication that Mr B’s personal data was actually viewed or accessed by a third party here, or that he has actually suffered

any harm or financial loss. And, in my view, the chances that the contents of the email happened to be intercepted, accessed or viewed by a third party and the contents then used to carry out fraud strikes me as being rather remote (although not zero). I should add that Mr B may want to delete the e-mail in question (if he has not done so already) if he is concerned about his inbox being accessed by a third party or he should ensure that he has two factor authentication on the account in question.

Nonetheless, Mr B is clearly concerned that his personal data was contained within an attachment that was contained, as far as I can see, in an unencrypted email. And looking at the attachment in question, it does contain a fair amount of Mr B's personal information that could potentially be mis-used by a third party. Therefore, to put things right, I think it's fair that TSB pay Mr B £30, so that, should he wish to do so, he can apply for a protective registration with Cifas as a precaution. Doing this will mean that, for a period of two years, any organisation that uses Cifas data will be aware that it needs to pay special attention, if it receives any applications for products or services that include Mr B's details. Although I would add that Mr B should do his own research about how a protective registration works first, if he does apply for one.

Finally, I note that the main reason why Mr B has complained is because he is concerned that TSB has sent an email unencrypted, and he says that TSB should change this process. However, it is beyond the remit of this service to dictate to TSB how it should operate, so that is not something that I would be able to do here. I'm limited to considering if TSB did something wrong - specifically in relation to Mr B - and whether it needs to do something to put things right for Mr B.

If Mr B remains dissatisfied with TSB's processes regarding how it handles personal data, then this is something he could potentially raise with the Information Commissioner's Office.

Putting matters right

To put things right, I require TSB to pay Mr B £30, so as to cover the cost if Mr B chooses to apply for a protective registration with Cifas.

My final decision

Because of the reasons given above, I uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 7 November 2025.

Thomas White
Ombudsman