DRN-5855235

The complaint

Miss C complains about problems when trying to access her online account with National Savings and Investments (NS&I).

What happened

Miss C holds a premium bond account with NS&I.

In June 2025 she experienced problems trying to access her online account using the password she'd used previously (albeit it seems it hadn't been used for some time). She spoke to NS&I about the difficulties she was experiencing. The agent she initially spoke to thought he'd managed to resolve the problem. However, when Miss C tried to log into her account later on, she experienced the same difficulties.

She called NS&I again. It asked Miss C to attempt to log in whilst it was on the phone to her, but she received the same error messages. It transpired that owing to NS&I's updated security system, it required Miss C to use a two-factor authentication. In order to set this up, Miss C required a one time passcode (OTP). And whilst it seems NS&I's system tried to call Miss C and provide an OTP each time she tried to access the account, due to a 'call guardian' on her phone, the calls didn't go through. In an effort to resolve the problem, NS&I suggested that Miss C could ask her phone provider to add the telephone number to a "whitelist", to prevent future calls being blocked. It also asked Miss C if she had a mobile phone number or another phone that she could use to prevent the same problem from happening. She confirmed she didn't.

Miss C wasn't happy with the explanations she was given and the actions NS&I expected her to take to resolve the problem. It logged a complaint on her behalf.

NS&I called Miss C about her complaint on 11 June 2025. She queried why NS&I couldn't send an OTP by email. It repeated that the problem was being caused by Miss C's phone provider (due to the call guardian that was in place). Miss C said the problem was NS&I's not hers and she said she wanted to escalate her complaint.

NS&I sent its complaint response soon after. It explained that it had introduced changes to its system security features in line with the Financial Conduct Authority's (FCA) guidance on enhancing security for its customers. The changes it made were specifically aimed at reducing fraud during the authentication process. It acknowledged Miss C's frustration given the problems she'd experienced and said it had asked its technical team to look into things. However, it didn't think it could be held responsible for the fact that a third-party call blocker prevented Miss C from receiving the OTP. It again explained some of the steps Miss C could take to prevent this in future, such as contacting her phone provider (so that calls relating to an OTP could come through). Alternatively, she could transact by completing one of its online forms or by calling its customer helpline.

Miss C wasn't happy with NS&I's response, so she complained to the Financial Ombudsman Service. Her complaint was allocated to one of our Investigators.

When considering Miss C's complaint, our Investigator asked her whether she'd been able to contact her telephone provider as NS&I had suggested. Miss C confirmed that her telephone provider wasn't aware of the existence of a "'whitelist". In any event, she said, amongst other

things, that as her phone had been set up to prevent scam calls from coming through, she had no intention of getting her provider to lift this facility.

Overall, the Investigator didn't think that NS&I had treated Miss C unfairly – especially as it had suggested alternative ways that she could access her account.

Miss C didn't agree with our Investigator and made a number of points in response. Those included:

- Her phone provider said there was no such thing as a "whitelist". Miss C felt NS&I had misinformed us.
- NS&I should have more ways to send her a two-factor authentication – such as by email.
- NS&I needed to sort out its faulty system and not pass the problem back to her.
- She questioned who would compensate her if she lifted the blocker and was subsequently scammed before it was reinstated.

As no agreement was reached, the complaint was passed to me to determine.

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.

From all the evidence I've seen and heard, it's clear that this situation caused Miss C frustration. And given that she simply wanted to access her own account, in her own time, I can entirely understand her position.

However, it's important to say at the outset that it's not my role to tell a business like NS&I how it should operate. So, that means I can't direct it to communicate with its customers in a particular way. And neither can I say what security measures it should put in place to protect its customers' accounts. They're matters for NS&I to decide using its commercial judgement.

But it is my role to determine whether NS&I did anything wrong in its handling of this matter and whether it otherwise treated Miss C fairly and reasonably. I've given this very careful thought.

At times I think NS&I could have given Miss C clearer explanations in response to some of the points she raised. For example, on more than one occasion during her calls she asked why it couldn't send her an OTP by email. I think that's a reasonable question. But I didn't hear NS&I specifically respond to that point and it simply repeated that Miss C would need to contact her phone provider. I think the lack of response here could have given the impression that NS&I wasn't listening to what she had to say or working with her to find a solution that worked for her.

There were other points during the various calls where Miss C appeared unclear about how the OTP process worked in practice. For instance, she seemed to be under the impression that she'd have to temporarily lift the entire blocker on her phone to allow NS&I's calls through. And she questioned how an OTP could be sent to her phone, if for instance, she was in the middle of a call to NS&I. She also suggested her phone didn't have a queueing system. I suspect the point that NS&I was trying to make was assuming she'd added the number to the "whitelist"(meaning that her phone provider could adjust her system so that it allowed calls from NS&I, but not the other numbers she'd blocked) whenever Miss C tried to access her online account it would then send a code to her phone via an automated call. Also, as far as I'm aware, NS&I didn't need to send Miss C an OTP while she was on the phone to it – as it could presumably (and indeed had already done so) verify her identity by

other means during a call. But NS&I didn't address this point head on when speaking with Miss C.

I don't know if earlier and clearer communications would have made a difference to how well received NS&I's suggestions for accessing Miss C's account would have been. I say that because Miss C was clearly of the opinion that this was NS&I's problem – not hers. But I still think these would have been additional reasonable steps for NS&I to take, especially when it was clear that Miss C was frustrated by its responses.

Turning now to the crux of Miss C's complaint.

These days, in the wake of increasing risks from fraud and scams, it's not unusual for financial businesses to update their systems and processes to try and stay abreast of emerging issues. That's what happened here. Previously, Miss C used a password to access her account. But when she attempted to log on earlier this year (having apparently not done so for a while) NS&I had updated its security systems. So, it now requires customers to use a two-factor authentication when logging in online. This is common within the financial services industry.

In its complaint response, NS&I explained the background to it updating its security systems. As far as I'm aware, the FCA's guidance was largely introduced on the back of other changes to the Payments Services Regulations (in 2017) which introduced rules that focused heavily on strong authentication methods. As I've mentioned, NS&I introduced a process which involved sending customers an OTP by text message or an automated call. Again, that's a similar process to those that other financial businesses now use. And I imagine for many customers it works quite well.

However, it seems that due to Miss C having a 'call guardian' in place NS&I's automated calls couldn't get through. And she said she didn't have a mobile phone, so NS&I couldn't send her a text message. As I've said, not being able to access her account in the way she wanted clearly caused Miss C a great deal of frustration. Especially when NS&I suggested that she should ask her phone provider to "whitelist" the number to allow calls through. As far as Miss C is concerned NS&I's system is faulty. So, again she doesn't think the onus should be on her to sort out the problem. I can appreciate Miss C's point but that doesn't mean NS&I did anything wrong. For the reasons I'll now outline, I'm satisfied it acted fairly and reasonably overall.

I accept Miss C's evidence that her phone provider – or the supplier of her call guardian - doesn't offer, or wasn't aware of, a "whitelist" facility. But I don't agree that NS&I misinformed us. Apart from what NS&I itself said, from my own research, I've found the following:

" *you can whitelist telephone numbers so they get through call blockers by using the whitelist feature on your phone or by using call blocking services that allow you to manually add trusted numbers to an "allow" list. Many modern call blockers operate on a whitelist system, meaning they only allow calls from numbers you've designated to get through, blocking all others by default".*

It appears that Miss C's phone provider may be something of an outlier here. I say that as the whitelist facility is something that, as far as I'm aware, most phone providers offer, although they may use different terms such as VIP or trusted list.

I don't think NS&I could have known in advance whether it was something Miss C's phone provider offered or not. But given that it seems to be a fairly common feature, I think NS&I made a reasonable suggestion in the circumstances.

Further, when it became clear that this may not be a facility that Miss C could/would use (and she didn't have a mobile number or other phone to use) I think NS&I acted reasonably by exploring other ways that Miss C might access her account. For instance, it said that she

could continue to transact by completing one of its online forms or by calling its customer helpline. I found both of those to be suitable alternative methods in the circumstances.

Miss C's gone as far as saying NS&I needs to sort out its "*faulty"* system, rather than passing the problem back to her. But I've seen no persuasive evidence that the issues Miss C described arise from a fault with NS&I's system. Rather it seems to be incompatible with Miss C's call guardian, unless proactive steps are taken to amend the call guardian and allow the calls through.

In summing up, I entirely appreciate that this matter caused added difficulties for Miss C. And whilst I can understand why she may not welcome some of the additional steps NS&I recommend she take - that in itself doesn't mean NS&I acted unfairly or unreasonably. I say that especially because these steps were geared towards safeguarding the security of NS&I's customers' accounts. Such security measures are introduced for all customers to try to protect them from scams and particularly those conducted online via the customer authentication process. In those circumstances I don't find that NS&I's actions have been unfair or unreasonable.

My final decision

I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss C to accept or reject my decision before 5 January 2026.

Amanda Scott
Ombudsman