DRN-6158689

The complaint

Mr S complains that Nationwide Building Society has declined to refund him for transactions he didn't make. He also complains that they closed his bank account without telling him.

What happened

Mr S is represented throughout this complaint. For ease I'll refer to all correspondence as coming from Mr S.

Mr S had two accounts with Nationwide.

He says that between 18 July and 24 November 2024, there were hundreds of unauthorised transactions on his account made via a digital wallet token, totalling just under £4,000. Mr S says he only became aware of this when he tried to withdraw the money from his account in branch. He reported the matter to Nationwide who investigated the transactions.

Mr S says that between May and August 2024, he didn't have access to his two mobile phones. He advises they were confiscated by his school, and that's how he believes the disputed transactions were carried out.

Nationwide declined to refund Mr S because they thought Mr S authorised the transactions. Nationwide say the evidence showed the transactions were authorised using Mr S's genuine device. And during the period the disputed transactions were carried out Mr S was accessing his online banking using his biometrics. After the investigation, Nationwide also decided to close Mr S's accounts.

Mr S says he didn't have access to his online banking from March 2024 and denied it was him accessing the account. He also said Nationwide didn't let him know the outcome of the fraud claim or that they were closing his accounts. After raising these complaints with Nationwide, Mr S wasn't satisfied with their response so referred his complaint to our service.

One of our Investigators reviewed Mr S's complaint and they thought Nationwide had acted fairly in declining Mr S's claim. They thought this because:

- The evidence showed the transactions were made from Mr S's genuine device.
- His bank account statements show a number of faster payment transfers to new payees requiring online banking or banking app authorisation for an initial payment suggesting Mr S was in possession of his genuine device.
- Mr S's online banking was accessed on 20 July on his registered device and there's no plausible explanation as to how this happened without Mr S's knowledge suggesting Mr S was in possession of his genuine device.

Nationwide provided evidence of a letter sent to Mr S's address and call notes of attempted calls to Mr S's registered number to discuss the fraud claim and account closure. Our Investigator accepted Mr S says he didn't receive these but couldn't see that Nationwide were at fault for this.

Nationwide didn't respond to our Investigator's view. But, Mr S disagreed. He says he didn't authorise the payments and the fact that his device made the transactions does not prove that he personally carried out or consented to the disputed transactions. He believes his card

details or authentication credentials were compromised. He further said that he had not "knowingly" set up any new payees on his online banking and he denies "knowingly" accessing his online banking during the disputed time period. Mr S mentioned he was concerned that he had seen others on social media sharing similar experiences and this had been overlooked.

So, Mr S's complaint has 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.

I know this will disappoint Mr S, but having reviewed the evidence, I won't be asking Nationwide to do anything further and I'll explain why.

Generally, a bank is entitled to hold a consumer liable for authorised transactions, and the bank is liable for unauthorised transactions. Those rules are set out in the PSRs 2017. The regulations say that Nationwide must prove that the payment transactions were authenticated.

Nationwide has provided evidence that shows the transactions were carried out via a digital wallet token first registered on Mr S's device on 10 February 2024. Nationwide have explained that the two ways in which the card can be added to a digital wallet is via the banking app or by the digital wallet itself. And there's no evidence of Mr S adding the token via his Nationwide app so it must have been through the digital wallet.

I've seen evidence that Nationwide can show that two-factor authentication (where the card holder authorises adding the card through the app or through a one-time passcode sent to the cardholder's registered phone or email) was required for a 'card not present' payment on the same day to activate the digital token for the first time. A large number of transactions were carried out using this digital wallet token prior to the disputed transactions. Mr S accepts these payments were genuine.

So, I'm satisfied the payments were properly authenticated, but this on its own isn't enough to say Mr S consented to the payments using the same token after 18 July 2024. But overall I think he did, I'll explain why below.

Mr S says his two phones were confiscated by his school between May and August 2024 so he can't have consented to the payments. I've thought about whether this timeline aligns with the technical evidence and I'm afraid it doesn't. I say this because the same digital token was used to complete transactions that Mr S accepts were genuine in June 2024. It's not possible that the device was both confiscated and being used to make genuine transactions in June.

I've also thought about the information and access a third party would need to make these payments without Mr S's knowledge. This includes access to Mr S's device, obtaining or guessing his device passcode and access his biometric information, all without Mr S realising. Mr S says he hasn't shared any of these details. So, given there are thousands of potential combinations of passcode, and it is generally accepted that biometrics are unique to individuals, I'm satisfied this isn't the most likely scenario. Moreover, as the transactions continued from August (when Mr S says he regained access to his phone) to November, the third party would need to continue to take the device for use regularly until November without Mr S knowing. I also find this unlikely.

There were also several bank transfers during the relevant period. Mr S confirmed he knew the names of the payees, and they included his family and friends. So, even if we accept that Mr S's phones were confiscated, I'm unclear why an unknown third-party would make these payments to people known to Mr S.

Finally, I've thought about the timeliness of Mr S noticing the regular debits to his account. The transactions were happening for four months before Mr S reported his concern. I find this surprising because each time the account balance was low, another deposit was made into the account indicating the user was aware of the balance. Additionally, the evidence shows Mr S used biometrics to log into his online banking during the relevant time. I also consider it would be unusual for a fraudster to use an account for everyday spending rather than withdrawing or spending the account balance quickly.

I acknowledge there is confusion about the model of phone that had the digital token registered. But, given Mr S accepts two phones were registered, and the audit log shows two phones, I'm persuaded on balance, these are the same devices.

I acknowledge Mr S says he has seen other people on social media sharing similar experiences to his which he feels supports his case. I understand why Mr S feels this is important evidence. But, I'm afraid this doesn't outweigh the evidence I've considered specific to Mr S's case and circumstances, which I've explained above.

Overall, for the reasons I've outlined, I'm satisfied Mr S authorised the transactions and therefore I can't fairly ask Nationwide to do anything further.

Finally I've considered whether Nationwide fairly notified Mr S about the account closure. I've seen evidence that Nationwide sent Mr S a letter to notify him his account was going to be closed. And they also attempted to speak with Mr S over the phone. I understand Mr S is unhappy he didn't receive the letter but it isn't Nationwide's responsibility to ensure it was delivered, so I can't say they acted unfairly here.

For the reasons I've outlined above I won't be asking Nationwide to do anything further.

My final decision

My final decision is that I don't uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 12 May 2026.

Cheryl Dior
Ombudsman