DRN-5882210

The complaint

Mr S complains that Nationwide Building Society ('Nationwide') declined to reimburse him when payments were debited from his account which he says he did not make or otherwise authorise.

What happened

The circumstances of this complaint are well known to both parties, so I will not go into every detail of what happened here. But in summary, a number of transactions were debited from Mr S's Nationwide account which he says he did not make or otherwise authorise. These included Apple Pay payments and open banking payments. Mr S said that his computer had been infected with a virus, so he thinks this is how an unknown third party was able to complete the transactions. He also pointed out that one of the payments took place abroad when he was in the UK. Mr S asked Nationwide to reimburse his losses on the basis that he didn't authorise the transactions, but it declined to do so.

Mr S complained to Nationwide about its decision to not reimburse him. It declined to uphold his complaint on the basis that its fraud team had reviewed the decision and found no errors in the conclusion that the payments were made or otherwise authorised by Mr S.

Mr S remained dissatisfied, so he escalated his concerns to our service where one of our investigators looked into what had happened. They did not recommend that Mr S's complaint should be upheld, on the basis that they thought the evidence suggested that they payments were made or otherwise authorised by Mr S.

Mr S did not agree with our investigator's findings, so the case has been passed to me to decide.

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 think it's important to explain I've considered all of the information provided by both parties in reaching my decision. If I've not reflected or answered something that's been said it's not because I didn't see it, it's because I didn't deem it relevant to the crux of the complaint. This isn't intended as a discourtesy to either party, but merely to reflect my informal role in deciding what a fair and reasonable outcome is.

The regulations relevant to this case - the Payment Services Regulations 2017 (PSRs) – set out what is needed for a payment to be authorised and who has liability for disputed payments in different situations. The starting point is that the Mr S would be responsible for authorised payments, and Nationwide would be responsible for unauthorised ones.

The PSRs specify that authorisation depends on whether the payment transactions were authenticated correctly – and whether Mr S, or someone acting on his behalf, consented to them. So, the relevant finding for me to make here is whether I think it is more likely than not

that Mr S made or otherwise consented to the payment in dispute. I have carefully considered this matter, and based on the evidence available to me I think it is more likely than not that Mr S made or otherwise authorised the transactions. This is because, in summary:

- The technical evidence shows that the transactions took place on the one device – a mobile phone. This device was added to his Nationwide account over six months before the disputed transactions. There was undisputed activity on this device before the disputed transactions. There is no evidence to suggest that any new devices were added. The same IP address was also recorded for both undisputed account activity and the disputed transactions. Mr S does not appear to reject that this was his device – and I think the evidence shows that it is most likely that it was.

- The Apple Pay token which was used for the relevant disputed transactions was also set up over six months prior to the disputed transactions and was used for most of Mr S's genuine Visa transactions from this point until the disputed transactions took place.

- Mr S said that he had his phone with him at the time of the disputed transactions and that no one else could have accessed it. Given that I have concluded that the transactions took place on his device, it does not seem likely that they could have been completed by someone other than Mr S. There is no point of compromise for that phone.

- The technical evidence also shows that biometric verification, which Mr S had already set up, was used to login to his online banking to move funds from his savings to his current account to fund the disputed transactions, and used to verify the open banking payments. Mr S told our service that no other biometric details were stored in his phone, so it seems most likely that this data shows he must have gone into his app to authorise these payments. Mr S also said that he has not shared his card details or secure banking details with anyone. Considering all of this, it is not clear how an unknown third party could have completed the actions to make the disputed transactions, even if someone had gained access to his device without him knowing – which seems highly improbable here.

- Mr S said that the fact one of the transactions took place abroad when Nationwide accepted the payment was made from his normal IP address in the UK shows that this was fraudulent, but I do not agree. The transaction which appearing to be processed abroad does not actually mean that it was physically made abroad. Transaction data can reflect as having taken place abroad due to the currency they take place in, or the location of the merchant. So, this does not persuade me that an unknown third party must have made the transaction abroad, nor does it evidence fraud here.

- Mr S has provided evidence that his computer was infected with a virus, and explained that he connected his phone to this computer. I accept there was some kind of malware on his system, but this does not lead me to conclude that an unknown third party could have gained access to his online banking on his phone. I say this because the transactions did not take place on his computer – the technical evidence shows they took place on his phone.

- There is no evidence to suggest that the malware did, or even could, transfer from his computer to his phone. Malware is typically written for a specific operating system – and it would be highly unlikely that a trojan written for Windows or macOS could be executed on an iPhone iOS. Furthermore, iOS is not known to execute code that

does not have a valid Apple digital signature. Furthermore, it is highly improbable that biometric verification could be impacted by the type of malware Mr S's computer recorded.

- I have also thought about the movement of the funds from Mr S's Nationwide account. Most of the payments went to his own account held with another financial firm, which I will call 'R'. From there, most of the spend that took place was to gambling sites. It is unclear why an unknown third party would move the funds to another account held by Mr S before moving them onwards, as this would give Mr S more time to notice the fraudster had gained access to his accounts and could have prevented the fraudster from gaining access to the benefit of the funds.

- The payments from his other account with business R were completed by card payment and online transfers. Some of them required additional verification in the R app. So for an unknown third party to have completed these series of transactions over the accounts they would also have needed the R card details, and access to the online banking on Mr S's device through biometrics or security credentials – as well as access to his device and Nationwide app.

- Many of the disputed transactions from R went to gambling sites. It would seem unusual for an unknown third party with unfettered access to Mr S's accounts to simply gamble the funds rather than take them without the risk of loss. Mr S also said he does not use gambling sites, but I have seen evidence to the contrary on this point.

So, when considering all of this, I think that it is most likely that Mr S made or otherwise authorised these transactions and so it follows that Mr S should be liable for them.

Mr S has said that Nationwide ought to have been aware that the pattern and value of spending was not in line with his everyday account usage. There are some situations in which I would expect Nationwide to intervene with payments which are unusual or out of character for Mr S's account. However, in order for liability to shift to Nationwide, I would have to be satisfied that there has been a loss – and that an intervention could have prevented this loss. Mr S has maintained that he was not the victim of a scam here, and as I have outlined above the evidence suggests that it is most likely Mr S consented to these payments. So, I cannot safely conclude that Mr S suffered a loss as a result of fraud – nor that Nationwide could have prevented it.

My final decision

I do not uphold this complaint and require Nationwide Building Society to do nothing further.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 13 May 2026.

Katherine Jones
Ombudsman