DRN-4105926

The complaint

Mr M complains that Nationwide Building Society did not refund a series of disputed transactions on his account.

What happened

Mr M says that on 14 December 2022, he was attacked and hit over the head between 2 and 3am. He says he lost consciousness and when he came to, he was walking along a street and bleeding. At some point he realised his phone and wallet had been stolen. Later on that day, he telephoned Nationwide to report this and at that point he found out there had been a series of transfers made to his own account with a third party I'll call 'X' that he did not recognise. These were for £500, £1,000, £2,000, £790 and £2,500. These funds were then withdrawn from his X account the next day as cash in increments of £250.

Mr M raised a disputed transactions claim with Nationwide and they issued a final response letter on 4 January 2023. In this, they explained that the IP address used to make the fraudulent transactions matched the same IP address used to access Mr M's online banking records previously. So, the transactions were completed in the same location he used to conduct genuine activity in. In addition, Mr M's online banking was accessed with no obvious point of compromise and the transfers went to another account in his name. So, they declined to refund the disputed transactions as they thought it was more likely he authorised the transactions himself.

Mr M referred the complaint to our service and our Investigator looked into it. They felt that the evidence showed it was more likely Mr M made or otherwise authorised the transactions as the IP address used was the same one he frequently used for genuine transactions. In addition, the online banking activity showed biometrics were used to start the log in process prior to the transactions occurring at both 2:48am and 3:04am. With no other evidence to support Mr M's version of events, they did not agree the complaint should be upheld.

Mr M disagreed with the outcome. He felt that other evidence, such as the fact a loan application was made in his name, which was unsuccessful, and an increase in the overdraft was also attempted around the same time as the fraud, should be an indication of fraudulent activity.

As an informal agreement could not be reached, 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.

Generally, Nationwide is able to hold Mr M liable for the disputed transactions if the evidence suggests it's more likely than not that he made or authorised them himself. This position is

confirmed in the Payment Service Regulations 2017 (PSRs) and the terms and conditions of his account.

The evidence provided shows the payments were made using Mr M's genuine mobile phone device. While this is important, it isn't enough on its own to say Mr M is liable for the transactions. Nationwide also has to show it's more likely than not that Mr M himself made or otherwise authorised the transactions.

Nationwide has said there was not a clear point of compromise for Mr M's mobile banking app and that the passcode was successfully used to set up the payment. Mr M has pointed out the passcode was changed so the compromise could have occurred there. I can see that biometrics were used to access Mr M's mobile banking at 2:48am and again at 3:04am. So it is possible that a third party used Mr M's biometrics to access the account, however they would have had to do so three separate times over the course of 16 minutes which I think makes the scenario less likely.

Nationwide has evidenced that the IP address used to make the disputed transactions was the exact same IP address that Mr M had used for a significant number of genuine transactions via mobile banking. The IP address relates to a "location" linked to the internet activity of devices or the network used in the transaction. Nationwide has therefore relied on this evidence to show the transactions were carried out in the exact same location Mr M had previously carried out genuine transactions so they thought it was more likely these transactions are also genuine.

On balance, I think it is reasonable that Nationwide has relied on this evidence. As such a significant number of genuine transactions relate to the exact same IP address, I think it's more likely this IP address is linked to Mr M. So, for the disputed transactions to have occurred at the exact same location, I think it is reasonable that Nationwide has therefore held Mr M liable for them. And I don't think the evidence relating to the biometrics being used to access the mobile banking changes this.

I've considered if there is any other evidence that can be relied upon. Unfortunately, Mr M did not approach the police prior to reporting the fraud with Nationwide and he did not visit a medical professional for his injuries. So, I don't have any evidence that could verify his version of events in more detail. I appreciate Mr M's comments that other activity occurred on the account which he feels is indicative of fraudulent behaviour. But I don't think the overdraft increase or attempted loan application counteracts the IP address evidence outlined above or gives additional context around what could have happened.

Having considered everything available to me carefully, I think it was reasonable that Nationwide declined Mr M's disputed transactions claim based on the evidence available to them at the time. And I don't direct them the refund the transactions in question.

My final decision

I do not uphold Mr M's complaint against Nationwide Building Society.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr M to accept or reject my decision before 22 December 2023.

Rebecca Norris
Ombudsman