DRN-4206694

The complaint

Mr S complains that Nationwide Building Society will not refund transactions he says he didn't make or authorise**.**

What happened

Mr S is disputing over £15,000 of transactions made from his Nationwide current account between August and November 2022. The transactions are a combination of online payments made using Mr S's card details and faster payments. Mr S says he was not someone who checked his online banking at all so could not have noticed sooner. He thinks someone was able to make these transactions by remote accessing his Wi-Fi. He's explained that his mobile phone had not been lost or stolen, and that it was protected by a passcode and biometric face ID.

Nationwide investigated the matter. Mr S says he was told he was going to receive a full refund as he'd been a victim of an account takeover, but then the building society declined the claim. It said the device used for the disputed payments is the same device that Mr S has used for other payments that he doesn't think are fraudulent.

Mr S complained. He said his account has clearly been taken over. In its final response letter, Nationwide said it didn't believe the spend to be indicative of fraud. It said some of the disputed card payments were authorised using Mr S's banking app and from the same IP address as genuine payments he'd previously made. It said it wasn't possible for Mr S's type of phone to be accessed remotely. It also suggested that Mr S had been logging into his mobile banking and would have seen the disputed activity on his account.

Unhappy with Nationwide's position, Mr S referred the complaint to us. He said devices can be remotely accessed and his phone and mobile banking had clearly been compromised. He said Nationwide had let him down, pointing out he'd never received any phone calls or text messages from the building society to confirm if he was making the disputed transactions.

Our Investigator considered the complaint. Initially she upheld it. She said Nationwide's evidence didn't show what devices had been registered and deactivated on Mr S's profile and that Nationwide's evidence refers to a different model of phone to the one Mr S says he owned during the period of the disputed activity.

Nationwide asked whether Mr S had reported this matter to the Police and asked to see some supporting evidence to show what type of phone Mr S was using. Mr S provided details of his mobile phone contract. He explained that he'd not reported the matter to the Police because he'd been told he was going to receive a full refund.

Nationwide provided more technical evidence, including records of when devices were added to Mr S's account profile in April 2022 and July 2022. Nationwide couldn't confirm specifically what model of device had been added on each occasion. But it said the device added in July 2022 was from an IP address that had been connected to Mr S's account before, and it referred to other logging in activities involving Mr S's card and PIN from the same IP address as the July 2022 device registration.

Our Investigator reviewed the evidence and changed her position. She said to register a device required a one-time passcode that was sent to Mr S's genuine mobile number, and she couldn't see how someone else could have completed these steps without Mr S being aware. She also noted the first disputed transaction happened around a month after a device had been registered. She thought it was unusual for a fraudster to not use an account straight away if they had gained access to it.

Mr S did not agree. He said it wasn't relevant that a one-time passcode was sent to his correct phone number to register a device because both times it happened before any fraudulent activity took place. He thought it was speculation to say that a fraudster would have acted sooner, suggesting that the transactions happening over a longer period of time could have been a way for a fraudster to bypass Nationwide's security systems. He said it was not possible for him to trick Nationwide's system into thinking he owned a different model of phone. He pointed out that no-one had told him where the money had actually gone, and it should be easy to see that he was a genuine victim of fraud if this was looked into.

As no agreement could be reached, Mr S asked for the matter to be reviewed by an Ombudsman. I issued my provisional decision earlier this month. In it, I explained why I was minded not to uphold the complaint. An extract of that decision is set out below:

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

Mr S is disputing payments made using his card details and faster payments made from his account initiated through a third-party provider. He's explained he didn't agree that these payments could be made and suspects that his account has been taken over, and his home Wi-Fi has potentially been hacked.

It's important to highlight that with cases like this I can't know for certain what has happened. So, I need to weigh up the evidence available and make my decision on the balance of probabilities – in other words what I think is more likely than not to have happened in the circumstances.

Whether a payment transaction has been authorised or not is important because the Payment Services Regulations 2017 (PSRs), which are the relevant regulations that apply to these disputed payments, explain that account holders will usually be liable for payments they've authorised and, generally speaking, banks and building societies will be liable for unauthorised payments. If Mr S made the disputed payments himself or consented that someone else could make transactions from his account on his behalf, it would not be fair to ask Nationwide to refund the money.

Looking at the steps that were required to make these payments, from what I currently have to consider, I can't see how an unknown third party could have obtained all of the necessary information to complete the transactions without Mr S's knowledge or involvement. I'll explain why.

Nationwide's technical evidence shows all the disputed card transactions were made online using Mr S's card details and that the faster payments were authenticated using Mr S's mobile banking. But the regulations relevant to this case say that this authentication is not, on its own, enough to enable Nationwide to hold him liable. Under the PSRs, Nationwide can only hold Mr S liable for the transactions made at a distance using his card details online if he authorised them or he acted fraudulently. Nationwide can only hold Mr S liable for the faster payments if he authorised them or if they happened because he failed with intent or gross negligence to comply with the terms and conditions of his account with Nationwide and

the obligations set out in the PSRs.

Nationwide is arguing that Mr S authorised the transactions made. It says that some of the disputed payments made using Mr S's card details were verified at the time using mobile banking and all of the faster payments were verified through Mr S's mobile banking. So I've thought carefully about the steps required to set up and verify payment through mobile banking.

The first piece of evidence Nationwide has raised is the process that must be followed to register a device to mobile banking. It has explained that to be able to enrol a device, one of the steps is for a one-time passcode to be sent to the mobile phone number it has on file. No new mobile device had been registered to Mr S's profile since July 2022. Although Mr S feels this activity is not relevant as it happened before any of the transactions in dispute took place, I disagree. I consider it is more likely than not that transactions in dispute were made with the involvement of a device that followed the above registration process. It would not have been possible to make these payments without validation processes that originally required interaction with Mr S's genuine mobile phone number.

It is unfortunate that Nationwide did not keep the data to show precisely which devices were registered to Mr S's account. The records it does have show the same brand of phone that Mr S had, but a different model. But I am not persuaded that this, in and of itself, is conclusive proof that the transactions in dispute are not connected to Mr S. This is because exactly the same details are shown for transactions that are not in dispute, including payments moving money to other accounts Mr S holds. This also means I cannot place much weight on what Mr S has said about not checking online banking at all as the technical evidence suggests that he did use it much more regularly than he's said.

Mr S has been clear that his phone has not been lost or stolen. He's explained it had biometric security protections and that his online banking details have not been written down or shared with anyone else. Against that backdrop, it is difficult to see how someone would have had the opportunity to steal Mr S's personalised log in information or gain access to a one-time passcode to register mobile banking on a device without his knowledge.

Nationwide has explained that two of the payments to a merchant I'll refer to as NWQ flagged on its system and were blocked. Nationwide's evidence shows both payments were released using mobile banking and biometric verification. What this means is that someone logged into Mr S's mobile banking at the time the payments were made and confirmed they were genuine.

*In addition, similar IP addresses appear in the bank's records multiple times and in connection to transactions and activities that are not in dispute. A payment made to another account Mr S holds was undertaken from an IP address that was also used to confirm a disputed payment to a merchant I'll refer to as 3D. Similar IP addresses have also approved disputed payments to a merchant I'll refer to as E*A.*

There were also multiple undisputed transactions between the disputed ones over a significant period of time. If the disputed transactions were made by someone else, I think

Mr S ought reasonably to have noticed them and raised this sooner with Nationwide. I'm not persuaded Mr S wouldn't have noticed such significant activity on his account given the amount of money involved and the fact that he regularly used the account. I'm mindful that Mr S's statements show that he was receiving incoming credits from loans and the bank's records show that he tried to extend his overdraft. Against this backdrop, I consider it to be more likely than not that Mr S was aware of how much money he had and how it was being utilised.

I am sorry to have to disappoint Mr S. This is not an easy message for me to give and I am mindful that it will not be an easy message for him to receive, but it is where the evidence that is currently available has led me. On the balance of probabilities, I can see no way for anyone else to have accessed Mr S's device or known his personal security information in order to have made these transactions. From the evidence that both sides have currently provided to me, I don't consider that Nationwide acted unfairly by holding Mr S liable for the payments in dispute. This means I am unable to agree that Nationwide should be required to refund them.

Responses to my provisional decision

Nationwide confirmed it had received my provisional decision and had nothing further to add.

Mr S didn't agree. He felt key points he'd mentioned had been ignored. In summary, he said when making a faster payment on the app it only tells you to confirm the payment in the app itself. He said his account was taken over and the person who was in it was able to press a button to verify the faster payment with no use of a verification code sent to his phone number.

He said that he tried to go through all of the payments in dispute but may have missed some. He was clear that all payments to these companies are disputed. He said his IP address would be the same if his Wi-Fi was hacked. He said his phone not being the same one that was registered on the account as making the payments should be conclusive proof that he didn't make the transactions. He added that Nationwide should have contacted him with this amount of money being spent in a short amount of time to confirm who was making the payments. He said Nationwide did not contact him once by text, email or phone.

He felt Nationwide had failed him on all aspects and that what Nationwide had said and provided was not conclusive proof and my position was only based on probabilities. He also referred to another complaint he'd made to Nationwide and said the building society had told him it had been passed to us as part of this case but it hadn't been mentioned. He concluded by saying Nationwide was not acting fairly by not providing the apology, compensation or full refund he believes he's entitled to.

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 done so, I'm sorry to have to further disappoint Mr S, but I'm afraid the points he's raised in response to my provisional decision are ones that I've previously thought about, but I formed a different opinion to Mr S.

Mr S insists that he didn't authorise the payments in dispute and is concerned that I have reached my position on probabilities. I do appreciate why he wants to know with certainty what happened. There's a lot of money at stake. But I should be clear at the outset that I can't know with certainty what happened here. And where there is such uncertainty, I must reach a decision on the balance of probabilities. In other words, I must consider the evidence that is available to me and reach a finding on whether this suggests it's more likely than not that these transactions were authorised.

In my provisional decision I said it would not have been possible for someone to make these payments without validation processes that originally required interaction with Mr S's genuine mobile phone number. This remains my position. I'm not saying the disputed payments were made using a verification code sent to Mr S's phone number each time.

I'm saying that Mr S's genuine mobile phone number was required as part of the process to link a device to his mobile banking app and no new mobile device had been registered to Mr S's profile since July 2022. In the circumstances that have been described to me, I'm still not persuaded that a third party could have added a device to Mr S's profile without him knowing.

Nationwide doesn't have the data to show precisely what devices were registered to Mr S's account. The records it does have show the same brand of phone that Mr S had, but a different model. I understand why Mr S feels this proves he did not make the transactions. But I disagree. This is because exactly the same device details are shown for transactions that are not in dispute, including payments moving money to other accounts Mr S holds. I can't see why a third party would have moved money to other accounts Mr S holds. I've thought carefully again about what Mr S has said about IP addresses being the same if his Wi-Fi was hacked. But I remain unpersuaded. I still don't agree that the wider circumstances suggest it is more likely than not that these transactions happened because Mr S's Wi-Fi was hacked.

Mr S is concerned that Nationwide didn't pick up on these transactions at the time. He's pointed to the amount of money being spent in a short amount of time. But the disputed transactions span many months, making it harder for Nationwide to detect a concerning, sudden pattern. In my provisional decision I highlighted that Nationwide has explained that two of the payments to a merchant I'll refer to as NWQ flagged on its system and were blocked. Nationwide's evidence shows both payments were released using mobile banking and biometric verification. What this means is that someone logged into Mr S's mobile banking at the time these payments were made and confirmed they were genuine, so I don't agree with Mr S's position that Nationwide didn't intervene at all. But regardless of whether Nationwide notified him of these transactions at the time or not, it wouldn't make a difference to the outcome I've reached here. I say this because I still consider it's more likely than not that Mr S authorised these transactions and so it's fair that Nationwide holds him liable for them.

Finally, I've noted what Mr S has said about Nationwide passing another more recent complaint to us to be considered under the same reference number. But this is not how our service works. Mr S would need to refer a fresh complaint to us separately about any new issues he would like us to investigate.

My final decision

For the reasons I've explained, my final decision is that I don't uphold Mr S's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr S to accept or reject my decision before 25 April 2024.

Claire Marsh
Ombudsman