DRN-4276333

The complaint

Mrs O complains that Nationwide Building Society ('Nationwide') debited transaction(s) totalling approximately £6,000 which she says she did not make or otherwise authorise.

What happened

In November 2021, a series of four transactions took place on Mrs O's account which Mrs O said she did not make or otherwise authorise. The transactions were card payments which took place on the same day, spread out over approximately six hours. They totalled approximately £6,000. The payments went to a cryptocurrency company and Mrs O said she has never had any dealings with cryptocurrency. Mrs O said that she thought someone had hacked into her mobile phone and made these transactions.

Mrs O said she was staying abroad with family at the time the transactions took place. She said she received messages from friends which informed her someone appeared to have hacked into her social media application. She could not get into the application, and contacted the social media platform. She then checked her online banking and noticed that she had transactions pending on her account totalling nearly £6,000. She said she was shocked and panicked and so contacted Nationwide.

Nationwide looked into what happened and declined to refund Mrs O. They thought it was most likely that she had made or otherwise authorised the transactions. In summary, they said this was because:

- The IP address for the disputed transactions matched the IP address Mrs O had used for undisputed online banking logins;
- The transactions were made on the same device as Mrs O had used for undisputed transactions;
- Mrs O said she had not clicked on any phishing email links or similar which could have compromised her details and allowed an unknown third party to make these transactions;
- They said they got in touch with her registered number to confirm the payments were her;
- They could not find any other point of compromise for the relevant details such that the payments could have been completed by someone else.

Mrs O was not happy, and complained to Nationwide who looked at what happened again and did not alter their original position. They suggested they set up a payment plan to help her repay what was owed, but Mrs O did not wish to do this. Mrs O said that she had children who would use her phone who could have clicked on a link which could have allowed someone to hack her phone. She said they also shared wifi with neighbours in the flat they were staying in abroad, as well as sometimes using public networks. She said she had emailed the cryptocurrency platform to report that she had been the victim of fraud. She spoke to one of their agents who said they could see money was sitting in the receiving account, and they would secure these funds. Unfortunately, despite numerous efforts from our service, we have not been able to get any further information about this from the cryptocurrency company.

Unhappy with Nationwide's response, Mrs O brought her complaint to our service. One of our investigators looked into what had happened and initially recommended that Mrs O's complaint be upheld and the disputed transactions be refunded with 8% simple interest. They also said they agreed with Nationwide's offer of £50 compensation in recognition of the distress and inconvenience caused when they didn't return a call they said they would.

Nationwide disagreed with this, and provided further evidence. Our investigator reviewed the new evidence and changed their opinion on the matter. In summary, they felt it was more likely that Mrs O authorised the transactions or allowed someone else to do so. This was because, in summary, Nationwide had shown that the person making the transactions must have done so from Mrs O's device, with access to information that it was unclear how an unknown third party would have access to, and no attempts were made on the account after the card was cancelled – which an unknown third party would not have known Mrs O had done.

Mrs O remained dissatisfied. In summary, she said she did not authorise the transactions. She felt the device ID could have been tampered with or hacked and her card details were stored on her phone so that she could easily make payments online. She thought her card details must have been cloned. She reminded our service that her social media had been hacked and she had been unable to get back into it. She was not sure how an unknown third party could have done this exactly, but she said she did get a random call, or her children may have clicked on a link or something. She said as she was staying somewhere that was not her home, there were people coming in and out who she did not always know so she didn't know if one of these people could have got her card details. She said she was ultimately confused and did not know how this had happened, but that she was not responsible for the transactions. She said she lost her handset before she travelled. Mrs O said that fraudsters had left a 1p pending transaction for ages which she thought was to see if her account was still active.

As no agreement could be reached, the case was 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.

Having done so, I have reached the same conclusion as our investigator and for broadly the same reasons. I'll explain why in more detail.

Generally, Nationwide can hold Mrs O liable for the disputed transactions if the evidence suggests that it is more likely than not that she authorised these payments or gave someone else consent to make them on her behalf. I'm satisfied from Nationwide's technical evidence that the payments were properly authenticated – Mrs O's genuine security credentials and card details were used to make the disputed transactions. But the regulations relevant to this case say that is not, on its own, enough to enable Nationwide to hold Mrs O liable. So, I need to think about whether the evidence suggests that it's more likely than not that Mrs O consented to these transactions being made. Having done so, I think on balance it is most likely Mrs O authorised these transactions. I'll explain why.

- The evidence suggests that the transactions took place on Mrs O's genuine phone. I say this because the technical evidence shows the device ID, IP address and phone number used to make the transactions matched those used for online banking logins and undisputed transactions. This means that Mrs O's genuine mobile phone, with the phone number she had on her account for numerous years prior to the disputed transactions, was used to make the disputed transactions.
- The transactions also took place on the same IP address as genuine transactions. It is true that an IP address can be shared, for example if two devices are on the same

router. So, the fact that Mrs O was sharing her wifi with her family and neighbours in the accommodation they were staying in could mean that more than one person would have access to the same IP address. But, given the surrounding evidence, this does not appear to be the most likely thing that happened here.

- Nationwide have also shown that the payments triggered additional checks by Verified by Visa, which required her to be logged into her online banking account to authorise the transactions. This was also done from the same device ID and IP address as undisputed transactions and logins.
- After Mrs O contacted Nationwide and they cancelled Mrs O's card, there were no further attempts to use her card. It seems unusual that an unknown third party who had compromised her details would have known when she would have cancelled the card – so it seems unusual that they did not try to further transact on her account.
- So, when considering all of this evidence against Mrs O's suggestions of how someone else could have made these transactions, I cannot say that I think these are the most likely explanations of what happened here. I've thought about the most likely scenarios from what Mrs O has told us. I'll work through the different scenarios in turn.
- Firstly, an unknown third party who was physically present in Mrs O's accommodation managed to get hold of her card and phone and make the transactions. This would explain how someone else could have done it on the same IP address – using the same router or the mobile data here would have looked the same. But this would have required the unknown third party to have found her card to get the long card number and security code, and also would have required them to somehow bypass any security to get into her phone, and any security to get into her Nationwide account which would have been either biometric security or her passcode, in order to use the device to make the transactions and to authroise them through her online banking application. They would have had to do this over a period of about six hours – so either would have had to take and replace her device without her noticing multiple times, or had it for the duration without her noticing its absence. Whilst this is not impossible, it does not seem most likely here.
- Secondly, an unknown third party managed to hack into Mrs O's device – perhaps due to one of her children clicking on something they shouldn't have, perhaps by some other means. An unknown third party did manage to hack into her social media somehow around the same time. But this explanation does not provide a clear point of compromise for Mrs O's long card number or her security code. So, the unknown third party would have had to have somehow hacked into Mrs O's device, and made the transactions on her device without her noticing. They would have likely had to guess the long card number and security code. Whilst her card details were saved on her phone, this appears to have been saved in faster payment settings rather than in an easily viewable part of her phone. The unknown third party with complete unfettered access to her phone and banking application would have been able to drain her accounts and use up any credit facilities within a short amount of time, but for some reason would have decided to take these funds over numerous hours when they could not have known whether Mrs O would have noticed. Again, I am not saying this is impossible – but it does not seem the most likely explanation of what happened here.

Having considered the available evidence the most likely thing that happened here is that Mrs O, or someone acting on her behalf, made these transactions. And so it follows that it would not be fair and reasonable to ask Nationwide to refund the disputed transactions – so I will not be doing so.

I also think the £50 award Nationwide have paid Mrs O is fair and reasonable in recognition of the poor customer service they provided her in not calling her back when they said they would – and so will not be asking them to do anything further here.

My final decision

I do not uphold this complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mrs O to accept or reject my decision before 28 April 2024.

Katherine Jones
Ombudsman