

complaint

Miss D complains that Nationwide Building Society ('Nationwide') closed her bank account and filed a Credit Industry Fraud Avoidance System ('CIFAS') marker against her name. She says she's been unable to open a student account with another bank and thinks Nationwide is responsible for this. She wants Nationwide to remove the marker.

background

Miss D had a bank account with Nationwide. In September 2017 a payment of £10,400 was made to the account. The same day a couple of attempts were made to transfer the funds away, but these along with Miss D's online banking facility were blocked by Nationwide as it had identified the activity on her account as unusual and suspicious.

The following day Nationwide was contacted by bank - 'S' from which the £10,400 payment had come. It said that its customer had been the victim of an email interception scam – the money had, in effect, been transferred fraudulently into Miss D's account. Nationwide investigated the matter, returned the remaining funds to S and informed Miss D that it was closing her account. It also placed a CIFAS marker against her name.

Miss D contacted Nationwide almost two years later in May 2019. She said she tried to open a student bank account, however, she was unable to do so. She was told that the reason for that was that Nationwide had placed a CIFAS marker against her name. She asked Nationwide to remove the marker, but it refused. Nationwide said it couldn't agree with Miss D that it had acted unfairly in this instance, or that it had recorded inaccurate information on her credit file. Unhappy with its response Miss D referred the matter to this service.

One of our investigators considered what had happened. She wasn't persuaded Miss D's version of events was accurate. She concluded that Nationwide had acted fairly. She didn't recommend that Nationwide do anything more to resolve Miss D's complaint. Miss D didn't accept the investigator's conclusions and asked that an ombudsman review the case.

my findings

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, my review of the evidence has led me to the same overall conclusions as those reached by the investigator and for broadly the same reasons.

The investigator wrote a detailed view that sets out in full the facts, considerations and the evidence. Both Miss D and Nationwide have read the investigator's view, so I won't repeat every detail here, only those which form the basis of my decision. However, I can assure Miss D that I've reviewed everything, including her comments and evidence. If I don't mention any specific point, it's not because I've failed to take it on board and think about it, but because I don't think I need to comment on it to explain what I think is the right outcome. I hope Miss D doesn't take this as a discourtesy; our rules allow me to do this. This simply reflects the informal nature of our service.

The bar for recording a CIFAS marker is a high one. If a business decides to file a marker it must have evidence and meet CIFAS's standard of proof. To meet the standard of proof the business must have: reasonable grounds to believe that a fraud or financial crime has been committed or attempted; and clear, relevant and rigorous evidence such that the business could confidently report the conduct of the customer to the police. This should be more than just a suspicion or concern.

I've considered the guidelines and weighed the information Nationwide had, as well as all the wider information available to me. And I find there was a sufficient basis for Nationwide to register the marker.

I understand Miss D disagrees. She has said that she was not aware of any funds crediting her account, she did not make the transfer request and she hadn't acted fraudulently. However, in this case Miss D's bank account received a credit of £10,400. The next day the payment was found to have been fraudulent – in the sense that the customer from whose account it'd been made had been tricked into making the payment to Miss D's account. I've no reason to doubt the investigation carried out by S or to conclude that both S and Nationwide had reached the wrong conclusion. That means that Miss D's account was used to receive fraudulent payments.

Nationwide has also provided evidence to show that on the same day attempts were made to transfer those funds out of Miss D's account. These attempts were made online, using Miss D's online banking details, memorable data and passcodes – some of the activity on the day was from an IP address which she had used to access her online banking before and as recently as a few days prior to the arrival of the fraudulent funds.

Nationwide spoke to Miss D the day after the funds had credited the account and notification of fraud had been received from S. During this call Miss D asked what would happen to the funds in her account. Nationwide informed her they'd be sent back to S as they were fraudulently sent, and that her account would be closed. During this call Miss D didn't deny this money was hers and didn't challenge or dispute the decision to close her account.

I understand Miss D says she didn't speak to Nationwide in September 2017. But I must account for the possibility that she may be saying this to try to distance herself from what had happened. It's quite possible she did speak to Nationwide on discovering access to her account had been restricted and payments requested out of the account were being refused. Having carefully thought about this I think it's more likely than not that it was Miss D who spoke to Nationwide in September 2017. I say this because;

- Nationwide's security verification was successfully passed;
- of course, I accept it's possible, as Miss D has pointed out that someone could've obtained all her personal and security details – especially because she kept these written down in her room, purse and mobile phone. This potentially could've made it easier for someone other than Miss D to pass Nationwide's security checks over the phone. But I also need to ask myself why a fraudster would call Nationwide? How would they have benefited from this? Whilst not conclusive on its own, it's also not something I'd typically expect a fraudster to do; and
- having listened to several calls Miss D has had with Nationwide and this service, I do think it's more likely it was Miss D who spoke to Nationwide in September 2017 not some unknown third-party.

Miss D is adamant she had no knowledge of the money paid into her account, but I'm not persuaded this is the case. Having reviewed the activity on Miss D's account I can see she didn't use her account much. Prior to the fraudulent credit arriving it appears when funds did arrive into her account, she knew how much was in account and only the exact amount was spent. With that being said Miss D had a zero balance, no overdraft facility, received a credit of £10 into her account the week before the large fraudulent credit was received but withdraw £20 the day after - this would suggest that Miss D had knowledge of the balance in her account.

I also note Miss D's online banking was accessed from multiple different IP addresses. She believes this supports it wasn't her. I appreciate the point Miss D is trying to make but this still doesn't prove she had no knowledge of the activity on her account. Whilst it's possible Miss D may not have physically attempted to transfer the funds out of the account herself I can't ignore that her online banking records also show a login on the day the funds arrived from the same device and IP address which she had used to access her online banking before and as recently as a couple of days prior to the arrival of the fraudulent funds.

Whilst Miss D later told our investigator she had lost her purse at the time. She couldn't provide her with specific details. She said she'd written down and kept all her personal information and Nationwide sign in details in her purse. She says it's possible this is how a third-party was able to access her account. I've not seen any evidence to support that Miss D had informed Nationwide of this at the time. This is not the behaviour I'd usually expect to see if someone had lost their purse containing potentially all their bank cards and, in these circumstances, specifically had their online banking details compromised – making Miss D's recent testimony less credible.

Taking all the above into consideration I don't think Miss D's actions feel like the behaviour of an innocent victim and the only logical conclusion I can draw from the above is that I think Miss D knows more than she has shared with Nationwide and this service about the activity on her Nationwide account. So, I can't say Nationwide acted unfairly in applying the CIFAS marker or unreasonably more recently in its refusal to remove it.

I don't have reason to doubt Miss D experienced difficulties in opening a student account with another bank in the way she describes. And this may be related to the CIFAs marker. But taking all the above points together – I think there would have been good grounds to report the events here to the police to investigate, and that Nationwide were therefore justified in placing a CIFAS marker against Miss D's name. It follows that I won't be directing it to remove the marker or pay compensation to Miss D.

my final decision

For the reasons I've explained, my decision is to not uphold Miss D's complaint.

Under the rules of the Financial Ombudsman Service, I'm required to ask Miss D to accept or reject my decision before 19 September 2020.

Sonal Matharu
ombudsman