DRN-2623744

The complaint

Mr B complained because Nationwide Building Society:

- recorded a marker against his name on the CIFAS anti-fraud database;
- closed his newly-opened accounts without notice;
- required him to provide photographic ID when he'd already taken it to a branch which had scanned it in; and
- then told him to email his photographic ID, even though Nationwide believed his identity had been impersonated, which he said wasn't secure.

What happened

On 23 April 2019, Mr B applied online to switch his current account from another bank to Nationwide. His daughter had referred him, because of the promise of £100 for both of them for the recommendation. During the process, the system invited Mr B to apply for a credit card as well, which he did. Mr B's applications were both approved online. The same day, Nationwide emailed Mr B and asked him to provide evidence of his identity.

The next day, 24 April, Mr B went to a branch with his passport and driving licence. The branch scanned in the information, and the same day Nationwide emailed to confirm Mr B's application to switch had been accepted.

But on 26 April, Mr B received a letter from Nationwide, dated 24 April. This said Nationwide had declined Mr B's applications because they'd received information that someone had impersonated him.

Mr B rang Nationwide straightaway about the letter. The call handler put him on hold and spoke to Nationwide's financial crime unit. She told Mr B that he'd have to go to a branch with photographic ID. Mr B pointed out that he'd already done that, and the branch had scanned in the information. He also asked what had happened to make Nationwide think another person had obtained his details, and also asked about his application. The call handler said Mr B would have to make another application, and wouldn't let Mr B speak to the financial crime unit direct.

The call handler put Mr B on hold again and checked again with the financial crime unit. She told Mr B that Nationwide couldn't tell Mr B what had triggered it because that would disclose Nationwide's checks. Mr B pointed out that this was worrying for him, because he didn't know what had caused the issue. And he was concerned that the information on CIFAS might cause problems for him.

The call handler also told Mr B that the branch hadn't sent on Mr B's ID, which it had scanned. She asked him to send his photographic ID by email to the relevant department. Mr B queried how Nationwide had processed his data, and said he wanted to make a subject access request. The call handler refused, saying Mr B could only make the request in the same email when he sent in his photographic ID. Mr B said he wanted to know that the

process used had been proper. The call handler said ‘*’I understand you keep telling me the same thing”* and said she couldn’t give him any more information.

Mr B said he’d contact the other department as the call handler had told him to, but he also wanted to put in a formal complaint straightaway. The call handler put Mr B on hold for a third time, and then filled in the complaint form. Mr B said he wanted to be sure that Nationwide’s process had been proper and just, and that his information had been processed properly. He pointed out that he’d initially been asked to take his ID into a branch for security reasons. He’d done this – but was now being told he had to email it. As well as having already provided this once, it was inconsistent and email wasn’t a secure or proper way of doing it. Mr B pointed out that the situation was inconvenient and distressing.

Mr B followed up the phone call with a complaint letter the same day. This set out that: Nationwide had shown inadequate process when it asked him to submit his ID and personal information by email, especially when it suspected his ID had been compromised;

The call handler had told him that the reason the financial crime department hadn’t received the scanned ID, which he’d provided on 224 April, was that the branch hadn’t emailed it. The use of insecure email for both of these jeopardised Mr B’s data;

Nationwide’s letter said ‘’*The information we have received **suggests** that your details may have been used by another person to impersonate you. We have made the decision to decline your application.’’* Mr B said he was disappointed Nationwide had failed to investigate or substantiate this suspicion. And he pointed out that CIFAS’s leaflet, which Nationwide had provided, said that if a CIFAS record is returned during checks, member organisations ‘’*must not simply reject an application…and they are required to carry out further investigation that the personal data provided on the application is correct.’’* Nationwide had failed to give Mr B an opportunity to provide clarification. Mr B had discovered that Nationwide had recorded the CIFAS marker on the day it had written to him, 24 April;

Mr B said he’d already experienced adverse effects of this. He’d had a card transaction with his other bank declined, needing further verification. And when he’d made a data subject request to CIFAS to find out about the marker, his identity authentication had been rejected.

In its final response letter to Mr B on 23 May, Nationwide said that it understood that Mr B’s complaint was that his application had been declined and he’d received a letter saying Nationwide needed to see ID. It also understood that Mr B was unhappy that Nationwide had left a mark on Mr B’s credit (sic) file.

This letter doesn’t tally with the complaint points which Mr B actually made on the phone call, or in his complaint letter. However, the essence of Nationwide’s final response was that it had acted correctly because there had been concerns about impersonation, and it had marked Mr B’s credit (sic) file as a security precaution. It said it had acted correctly in declining Mr B’s application.

Mr B wasn’t satisfied and contacted this service. He set out what had happened, and said Nationwide had caused him severe undue distress. It had implied there were problems with his financial standing, and he’d had to explain to his daughter why his application had been rejected. The marker with CIFAS had impacted his access to financial services. He’d also lost time and earnings, having had to visit the branch twice to provide proof of ID, and had wasted significant time phoning and dealing with Nationwide. Mr B pointed out that his complaint wasn’t about an application being declined, but about service. He wanted to have the information on which Nationwide had based its decision, and why it had thought someone had impersonated him. He also asked for compensation.

Our investigator didn't uphold Mr B's complaint. He said he couldn't provide the evidence why Nationwide had put the marker against Mr B's name, but he was satisfied that it had followed the correct procedures. He said the CIFAS marker was for protective purposes and had no impact on Mr B's credit file. The investigator also said that Nationwide was entitled to close an account under the terms and conditions. He said that Nationwide had said that as it had been able to verify Mr B's identity, he'd be accepted if he chose to apply again.

Mr B remained unhappy both with Nationwide's response and the investigator's conclusions. He said Nationwide hadn't acted with due diligence. It could have rejected the application, but hadn't done. And it could have verified evidence of his identity as part of the application process, but hadn't done this properly. By placing the marker, Nationwide had informed other financial service providers while in the process of verifying his identity evidence.

Mr B also disagreed because the investigator had said he hadn't been affected, when he had been. Mr B accepted that Nationwide's terms and conditions allowed it to close an account, but he didn't agree that Nationwide could do this based on some misinformation. So Mr B asked for an ombudsman decision.

My provisional findings

I issued a provisional decision on this complaint. Before doing so, I considered all the available evidence and arguments to decide what would be fair and reasonable in the circumstances of this complaint.

I asked Nationwide for much more information, including copies of the applications; copies of all emails and letters; the phone call recording on 26 April and any other phone calls; why the final response referred to Mr B's credit file when it was a CIFAS marker which had been placed; and the full reason why Nationwide had concluded that someone was impersonating Mr B. Nationwide provided some of this, and I used the phone recording to set out the full details of this important call above. Nationwide said it did not retain copies of the correspondence, so I took Mr B's account of what happened as the most likely version of what happened here.

Whether Nationwide was right to place a CIFAS protective marker against Mr B's name

Impersonation and identity fraud are serious issues, as both Nationwide and Mr B agreed. And if someone has been impersonated, it's important that there is the protection of a CIFAS marker to prevent unauthorised access to the genuine person's finances. This protects the genuine consumer, in this case Mr B.

So Nationwide was right to take the threat seriously. In my provisional decision, I explained that I couldn't disclose the evidence which Nationwide said led it to believe Mr B had been impersonated. I wasn't persuaded by some of the reasons Nationwide gave, but some might have led to concerns. And I couldn't know the full reasons behind Nationwide's internal computer system which would have contained complex algorithms. So on balance I accepted that Nationwide probably had valid concerns to justify a protective marker for Mr B. I bore in mind that protective markers are to protect customers, so wouldn't necessarily have been a detriment to him, if Nationwide had dealt with Mr B properly in doing so.

Closure of Mr B's accounts

Sections 74 to 78 of the terms and conditions of Mr B's current account, and section 10 of the terms and conditions of his credit card, set out when Nationwide can close an account immediately. The wording is slightly different for the two products.

The current account wording referred to ‘*’exceptional circumstances”* and said this might include where ‘*’you have carried out (or we reasonably suspect you have carried out) illegal or fraudulent activity on the account.*’’

The credit card wording referred to *“if we reasonably believe it is necessary to prevent fraud or unauthorised access.”*

I accepted that Nationwide had concerns that Mr B might have been impersonated. So it was fair to register a protective marker, and to stop transactions on the new accounts. But Nationwide closed the accounts before conducting any investigation. What Nationwide told Mr B it needed was photographic ID – which in fact he’d already provided to the branch two days earlier.

I considered it would have been reasonable for Nationwide to have simply put a block on the two new accounts, and then investigated. And the problem was unlikely to have arisen anyway, if the scanned branch copies of Mr B’s ID had reached the records when he took them in on 24 April. So I found that it would have been reasonable for Nationwide not to have closed the accounts but simply stopped them pending investigation.

This wouldn’t have prevented the worry and inconvenience from issues around the protective CIFAS marker, but it would have avoided the situation where the 26 April call handler told Mr B that he’d have to apply all over again if he wanted the accounts.

Mr B had quoted CIFAS, which says that organisations mustn’t simply reject an application but have to carry out further investigation that personal data provided is correct. But the CIFAS leaflet refers to situations where an organisation has checked CIFAS and found an existing marker. That wasn’t what had happened here. But I did agree that Nationwide should have investigated before closing Mr B’s new accounts – because that would have been fair and reasonable.

Data protection

Mr B’s original complaint to Nationwide complained that it had failed to treat his information with due care, or to process his information with due care. He said that the practice of using email internally (when the branch should have emailed his scanned ID) and externally (when it asked him to email his ID despite having received it already) exposed him to increased risk of his identity being compromised.

It’s not uncommon for a financial organisation to use email communication internally and externally – depending on the steps they may take to ensure this is secure, for example encryption etc. But by not reassuring Mr B and explaining what it had done and why it had to do it this way, it would only have added to his worries.

Nationwide’s customer service towards Mr B’s concerns – call handling and final response

Looking first at the 26 April phone call, I found that Mr B was very patient and measured with the call handler. It was entirely understandable that he was very worried and concerned. He’d initially been told the applications had been accepted online. He’d also promptly taken photographic ID to a branch. But he’d then had the acceptance overturned, and even more worryingly had been told that there had been evidence he’d been impersonated. I found that anyone would be worried at this.

I quite understood that Nationwide couldn’t give full information about all its security processes to Mr B, or to any customer. No bank can disclose such information without

jeopardising security, and Mr B recognised the need for security during the 26 April phone call. But in terms of customer service, I thought Nationwide could have been much more helpful here.

It was completely understandable that Mr B was worried that someone might have impersonated him. Nationwide didn't allege, either at the time or since, that Mr B himself had done anything fraudulent. So it would have been appropriate for Nationwide to be sympathetic and reassuring towards Mr B. That wasn't the tone of the call. And at no point did the call handler reassure Mr B that his data wasn't in danger or that things could be sorted out and put right. Nor did she seem to understand what Mr B meant when he pointed out that he was now being asked to send his personal data by insecure email.

Certainly the call handler set out Nationwide's policies and what Mr B had to do next, and she referred to the fraud department when she didn't know the answer. But the tone wasn't helpful and it was clear she wanted to get rid of the call. I don't agree, for instance, that Mr B ''kept telling her the same thing.'' I consider that Mr B might not have had to make a complaint if this call had been properly sympathetic and explanatory.

Going on to look at Nationwide's final response letter in connection to the problems here, I found that this failed to deal with the points which Mr B had identified in the 26 April phone call, or in his complaint letter. Mr B made intelligent and sensible points which I've set out above, about the use of email, and lack of investigation before placing a CIFAS marker. But the final response letter didn't deal with any of this. Instead it justified placing a credit file marker against Mr B – which it hadn't done – and talked about the right to decline an application. I considered that the person who wrote the letter couldn't have listened to the 26 April call recording, or read Mr B's complaint letter to the bank.

Impact on Mr B

Nationwide had argued that the situation was rectified in less than a week. I didn't have evidence about when the marker was removed, but Nationwide didn't tell Mr B that the marker had been removed until the final response letter dated 23 May, which was almost a month after it was recorded on 24 April. And the final response, as I've set out above, mistakenly referred to marking Mr B's credit file, rather than a CIFAS marking. So even this wouldn't necessarily have been reassuring.

In Mr B's complaint letter to Nationwide on 26 April, he set out that there had been adverse effects. He'd had a card transaction declined needing further verification. And when he put in a subject access request to find out about CIFAS, his identity authentication had been rejected. So I accepted that there were practical impacts of the marker.

But I considered the greater impact was the frustration and worry which was caused by Nationwide's poor service. Anyone would be worried to think they'd been impersonated and their personal data at risk. Even after Mr B had produced identification, thus proving there hadn't been impersonation, Nationwide didn't reassure Mr B or act kindly towards him.

I considered that the failure in Nationwide's procedures made that distress worse. The branch to which Mr B had promptly taken his photographic ID hadn't put this scanned information on Mr B's records. The phone recording implies that the systems were such that branches had to email this scanned document, rather than it uploading onto Nationwide's system. But whether it was a branch failure or a system issue, it shouldn't have been necessary for Nationwide to have to ask Mr B for his ID again, two days after he'd already provided it. And it's entirely understandable that Mr B would have been upset, worried and frustrated when Nationwide told him on 26 April that he'd have to email his ID.

To summarise, I considered that although Nationwide couldn't be said to have acted wrongly in recording a protective CIFAS marker, it did provide very poor customer service around this. It closed his accounts when it could have blocked them and investigated. It failed to transfer the scanned photographic ID which Mr B had provided at branch as requested – which it later said was the evidence it needed that Mr B hadn't been impersonated. Above all, it didn't deal kindly or helpfully with Mr B either in the 26 April phone call, or in the final response. And the final response bore very little resemblance to Mr B's 26 April written complaint. So I considered that Nationwide should pay Mr B £300 compensation for this poor service.

I said that I was aware that Mr B and his daughter would have received £100 each if the current account switch had gone ahead. When I wrote my provisional decision, I didn't know whether this had been paid, as the account was opened then closed. I said that both parties should confirm this in their responses to my provisional decision.

Responses to my provisional decision

Mr B accepted the provisional decision. He confirmed that neither he nor his daughter had received the £100 each which they'd have received if the transaction had gone well. He asked that Nationwide should pay both of these promised amounts.

Nationwide also accepted the provisional decision, and said it was willing to pay Mr B £300 compensation with an additional £100 in lieu of Mr B's referral payment. It said that CIFAS didn't appear to show when a marker had been removed. But it said it had conducted a search and there were currently no markers against Mr B's name.

This service has spoken to Nationwide separately about Mr B's daughter's referral payment. So, as we've told Mr B, this decision relates just to Mr B's complaint and his own compensation.

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 reconsidered all the available evidence and arguments, I see no reason to depart from my original conclusions.

My final decision

My final decision is that I uphold this complaint and I order Nationwide Building Society to pay Mr B:

- £300 compensation for its very poor customer service to Mr B, which caused him distress and inconvenience; and
- £100 which Mr B would have received as his share of the account-switching incentive.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr B to accept or reject my decision before 24 March 2021.

Belinda Knight
Ombudsman