DRN-4558333

The complaint

Mr E complains that Bank of Scotland plc (BoS) used contact information he'd provided in connection with another account with a different bank, (who I will call 'X'), for the purposes of his Halifax account.

What happened

In October 2023 Mr E opened a Halifax bank account; Halifax is a trading name of BoS.

Mr E went to set up mobile banking and was advised Halifax would send him a text message. Mr E never received this text and called Halifax to resolve things. It was later established that this text message was sent to a contact number Mr E hadn't provided in connection with his Halifax account. And Mr E was told he was unable to update his contact number over the phone. Mr E then had to attend a Halifax branch the following day to verify his new contact number. Mr E was unhappy with this and raised a complaint.

Halifax responded to his complaint and explained that when he'd opened his Halifax account it had used an existing profile. It explained Halifax and X were both part of the Lloyds Banking Group (LBG) and it would use the same profiles and contact information for customers across the group. It also advised that whilst Mr E had provided a new contact number when he'd opened his Halifax account, it wouldn't add new contact information to existing profiles within the LBG following the opening of a new account online as a fraud prevention measure.

Mr E remained unhappy as he didn't feel the LBG should have retained his contact information given his account with X was closed in May 2023. Mr E felt there had been a data breach and the businesses ought not be sharing this information. Halifax explained that the LBG would hold information for ten years regardless of whether the account was closed unless it received a specific request from Mr E to remove his personal information from its records – which it had not. Mr E then brought his complaint to our Service.

Our Investigator looked into things but didn't uphold the complaint. They said it was fair for Halifax to ask Mr E to verify his details and noted that Halifax's privacy notice does explain that the LBG uses the same details across products.

Mr E disagreed. He stressed that he didn't think they had the right to hand over the information between the separate businesses in this way. He noted Halifax hadn't told him it would link the data to his LBG profile. It didn't give him any indication that it would use pre-existing contact information. This meant he had no opportunity to check or amend his contact number which he thinks he ought to have been given. So, the complaint was passed to me to consider.

I asked Halifax for more information about this complaint. It explained:

- Halifax sent two text messages to his old contact number, neither of which was delivered.

- During the call with Mr E, Halifax couldn't update his contact number because it couldn't verify his identity due to the lack of account activity. It explained to Mr E that to update his contact number he could attend branch or it could send him a passcode via post.

After reviewing things, I thought it was likely I'd reach a different outcome to the Investigator, so I issued a provisional decision to ensure both parties had the opportunity to respond before a final decision was made. In brief, I said that Halifax's communication surrounding its processes was lacking and I suggested it pay Mr E £100 compensation.

Both Mr E and Halifax accepted my provisional findings and made no further representations. So, I am now in a position to issue the final decision on this complaint.

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.

I'd like to clarify that this is a complaint against BoS. And whilst it may be part of the wider LBG, X is a separate firm. So, if Mr E has concerns about X's actions in relation to his personal information, then he will need to raise a complaint with it directly. I cannot consider whether X's retention of his personal data was fair. In this decision I can only consider the actions of BoS trading as Halifax.

Firstly, I'd like to be clear that it's not my role to decide whether there has been a data breach here. This would be for the Information Commissioner's Office which regulates compliance to data protection laws in the UK. My role is to decide whether I think BoS has acted fairly in the circumstances and to consider the impact on Mr E if it did not.

Broadly speaking, there are three parts to Mr E's complaint:

1. That he wasn't able to update his contact number over the phone.
2. That Halifax accessed his information from his account with X and didn't tell him this.
3. That Halifax didn't accept the new contact information he provided in his account application.

Halifax has explained that the reason Mr E wasn't able to update his contact number over the phone was because the account was new. This meant it didn't have any account activity information it could use to assist with verifying Mr E's identity to a high enough level to allow this change. Taking into account that Halifax then offered Mr E two alternative solutions to enact this change, I'm satisfied it was following its security procedures here and that this was reasonable in the circumstances.

Halifax has also explained that its process of accessing contact information from the LBG and not accepting new telephone numbers is a fraud prevention measure. Banks and building societies have an obligation to try and keep their customers' accounts safe and prevent fraudulent transactions. And the bank is under a legal obligation to monitor customer accounts and carry out due diligence checks in order to prevent money laundering and other types of financial crime.

Whilst I understand the fraud risk here and the importance of safeguarding against this, it's not clear to me how these measures fairly account for when people who are not attempting to act fraudulently do change their contact information. And I think the key for me here is that there's been a lack of communication about all of this.

I'm satisfied Halifax's privacy policy does state that information is shared across the LBG. But I can't see that Halifax brought this to Mr E's attention in a clear enough way that he would have understood how this data sharing might impact him.

Had Halifax told Mr E at the point of application that it would use contact information held across the LBG and that it might not immediately accept changes of contact information given as part of the application process, then Mr E would have at least understood what might happen – including the extra steps he may have needed to take – and why. As it stood, Mr E finished his application process with what I think was a reasonable assumption that Halifax held his correct contact information. That turned out not to be the case through no fault of his own.

I think Halifax's failure to communicate with Mr E at the application stage to explain its process has created misunderstanding which has led to unnecessary frustration and confusion. Ultimately, Mr E's expectations were mismanaged as he anticipated being able to provide his contact number and complete his registration process online, but he ended up having to attend branch (or wait for a passcode in the post).

As such I think Halifax ought to compensate Mr E and I think £100 fairly reflects the loss of expectation and frustration caused.

My final decision

My final decision is that I uphold this complaint and direct Bank of Scotland plc to pay Mr E £100 for the distress and inconvenience caused.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr E to accept or reject my decision before 12 August 2024.

Jade Cunningham
Ombudsman