DRN-4536134

The complaint

Mr F complains about Co-operative Bank Plc's ("Co-op") security processes for making online debit card transactions. In particular Mr F objects to the resetting of a password for two step authentication through an unencrypted verbal means over the phone.

What happened

On 7 November 2023 Mr F attempted to make a transaction online and was prompted to enter his security details. Mr F says after multiple failed attempts at this he rang Co-op and was advised to use an existing password – his memorable name - that is used for another function and that he should change it verbally over the phone. Mr F didn't wish to do that as he felt this was a breach of security best practice to provide his password to a person over the phone who already had his phone number, address, date of birth and other personal security data.

Mr F complained to Co-op about this and that he wasn't told that his memorable name was going to be used as his password for transacting online.

The Co-op advisor explained that when a customer enters the new password it disappears and is not stored on its system in full and is not visible to an adviser and that the password alone is not sufficient for a transaction to be processed as a customer will also have to enter a pass number sent via text. Co-op didn't uphold Mr F's complaint as there had been no error on its part.

Mr F was dissatisfied with this as he says he has been left with a re-used password which he believes is an inherent security weakness and that he can only change it by going through what he believes is an even less secure process. Mr F says this limits his ability to make any secure transaction where the secure payment password is a requirement and brought his complaint to this service.

Co-op have explained that for remote debit card transactions where the customers are not present, they need to complete a security process which involves verifying a purchase by using a full password in conjunction with a One Time Password (OTP) usually sent via text.

This process was implemented in late 2022 to ensure the security of consumer accounts and to protect against debit card fraud and in-line with regulatory guidelines. Co-op say it notified consumers via multiple platforms that its security process when making debit card transactions was changing and is stated on its website.

The password that is required going forward when making debit card transactions is the same as the customers memorable name already held with Co-op – unless the customer called it to change it to something else. Previously a customer was required to enter three characters from this password – rather than the full password.

One of our investigators looked into Mr F's concerns and didn't think Co-op had treated Mr F unfairly or had made an error as they were satisfied Co-op had informed its customers of the

changes in advance and were satisfied Co-op was acting within their best interests regarding its security processes.

Mr F also was unhappy with the way Co-op dealt with his complaint and its complaints process – but as complaint handling isn't a regulated activity our investigator explained to Mr F that we wouldn't be looking at this part of his complaint.

Mr F remains unhappy as he doesn't believe providing a password over the phone is secure and has asked for an ombudsman's decision.

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.

My role is to look at problems that Mr F has experienced and see if Co-op has made a mistake or done something wrong. If it has, we seek to put - if possible - him back in the position he would've been in if the mistakes hadn't happened. And we may award compensation that we think is fair and reasonable.

It might be helpful for me to say here that as we are not the regulator, I don't have the power to tell Co-op how it needs to run its business and I can't make Co-op change its security systems or processes – such as the security measures and procedures that it needs to have in place to meet its regulatory obligations. This simply is not something for me to get involved with, we offer an informal dispute resolution service and we have no regulatory or disciplinary role.

That said, from what I've seen I don't think Co-op have treated Mr F unfairly or acted unreasonably by implementing new security measures that it believes is in-line with regulatory guidelines for Strong Customer Authentication for the ongoing protection of its customers against fraud when making debit card transactions when the customer isn't present.

I'm satisfied from the information I've seen that Co-op gave its customers pre warning of the implementation of new security measures through different platforms such as letters and emails sent out as well as providing this information on its website. Within this information I can see Co-op explained what the changes were and what to expect – including that the memorable name would be the password used until it is reset - and why it was necessary to make the changes.

Furthermore, I'm satisfied that it has applied the same security measures for all its customers and that having listened to the phone call between Mr F and Co-ops advisor that it followed the correct process when Mr F called up regarding the transaction he wished to make and the process for updating his password. So I can't say that Co-op has treated Mr F unfairly or made a mistake here.

I understand it is not the implementation of these measures Mr F has an issue with, but rather that he doesn't believe the reusing of his password or memorable name or the process for changing this is secure. In particular, Mr F is unhappy that to change his password he needed to provide a new password verbally and unencrypted to a Co-op advisor over the phone who had access to other personal details.

As I've already explained above, it is not for me to say whether Co-op's security measures and processes meet best practice, but nevertheless the Co-op have explained that the new password provided by its customers when entered onto its system isn't stored in full and that

the password alone is not sufficient for a transaction to be processed as a customer will also have to enter a separate pass number sent via text. So even if the Co-op advisor did manage to remember Mr F's new password in full, my understanding is they still wouldn't have been able to transact without the second step authentication.

I appreciate Mr F feels strongly about Co-ops security processes not being best practice and the implications of this for the future security of his account and him being unable to transact online. But when looking at a complaint we look at what actually happened and not what might have happened. And in this case as I haven't seen that Co-op have made a mistake or that Mr F has suffered any detriment due to the implementation of its security processes and in particular for online debit card transaction he wished to make at the time. So it follows that I do not uphold this complaint.

My final decision

For the reasons I've explained, I've decided not to uphold Mr F's complaint against Co-operative Bank Plc.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr F to accept or reject my decision before 21 May 2024.

Caroline Davies
Ombudsman