

As you may have seen in the news, the Heartbleed Bug, an encryption flaw of OpenSSL, has affected many popular websites and services — ones you might use every day, like Gmail and Facebook — and could have quietly exposed your sensitive account information (such as passwords and credit card numbers) over the past two years.

OpenSSL is a very popular implementation of the SSL/TLS cryptography protocols used to encrypt many network communications, including secure web communications.

The FCB IT Department has been working diligently to test and verify all systems and servers in the bank and all vendors and 3rd party service providers, including online banking, to assess what implication this will have on our customers, communication, and the security of our data.

At this time we have determined that our security and data have NOT been compromised. With specific regard to online banking, the version of OpenSSL installed within the online banking environment was not vulnerable to this bug at any point. The currently installed version has not changed, and has never been vulnerable, and updates or patches have not been applied as a result of the public disclosure.

We will continue to monitor this situation and mitigate any threats as we become aware.

The article below has compiled information on other popular websites that might have been affected and may be worth your time to see if you should change passwords on other websites you may use.

<http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/>

Feel free to contact FCB at contactus@myfcbusa.com if you have any specific questions regarding the safety and security of your data.