April, 2014 - Choice Bank services not affected by OpenSSL Software Vulnerability ('Heartbleed")

On April 7, the OpenSSL organization publicized a new, critical vulnerability called “Heartbleed,” which is associated with certain versions of OpenSSL software. What is the potential risk? The vulnerability within OpenSSL could allow a remote attacker to expose sensitive data which may include user authentication credentials and secret security key codes. Basically, they had a bug in the memory handling part of their software known as the “TLS heartbeat extension”.

We have been in contact with our vendors who provide web-based services that we utilize to provide banking services to our customers and provide security here at the bank. **Our vendors have assured us that there has not been a compromise by this vulnerability.** We, along with our vendors, will continue to monitor the situation in conjunction with the security community and technology partners.

Technology changes constantly. There are unfortunately new security threats being posed to consumers and businesses every day. You can help mitigate these threats and help protect your personal information by taking precautionary steps like changing your passwords on a regular basis. Additional security tips can be found above on this Security Center page.

If you have any questions about your Online Banking service, please contact our personal bankers during our normal business hours (Monday-Friday, 9 am to 5pm) at 1-920-230-1300.