POODLE SSLv3.0 Vulnerability (CVE-2014-3566)

Based on recommendations from Red Hat, we will disable support for SSL v3 on servers that use SSL for encrypted connections (https).

Internet Branching:

We will disable support for SSL v3 on all Internet Branch servers. This action may result in some members who are using old web browsers (Internet Explorer 6, for example) being unable to connect to your Internet Branch. Older browsers may not have support for TLS 1.0 (and higher) and have been using SSL v3 to connect.

CAMS-ii:

We will also disable SSL v3 on CAMS-ii servers that use SSL encryption. This affects customers that access CAMS-ii in an online (hosted) environment where the CAMS-ii server is not installed in the credit union. Those customers that have their CAMS-ii server in their building do not use SSL for connectivity to CAMS-ii.

Individual Browsers:

Most websites will likely disable SSL v3 in the near future. However, you may disable support for SSL v3 in your browser, if desired. Mozilla has announced that Firefox version 34 (scheduled for November 25) will remove support for SSL v3. Google has stated that Chrome will be updated in the near future as well. Both may also have add-ons to handle this now.

Internet Explorer already allows you to disable support for SSL v3. Go to Settings (it may appear as a gear icon in the upper right corner of the browser), then Internet Options. In the Advanced tab, scroll to the **Use SSL 3.0** check box**.** Make sure that the check box is cleared/ unchecked. Click **OK**.