#36385

TO: **ALL CLEARING MEMBERS AND EXCHANGES**

DATE: **MARCH 12, 2015**

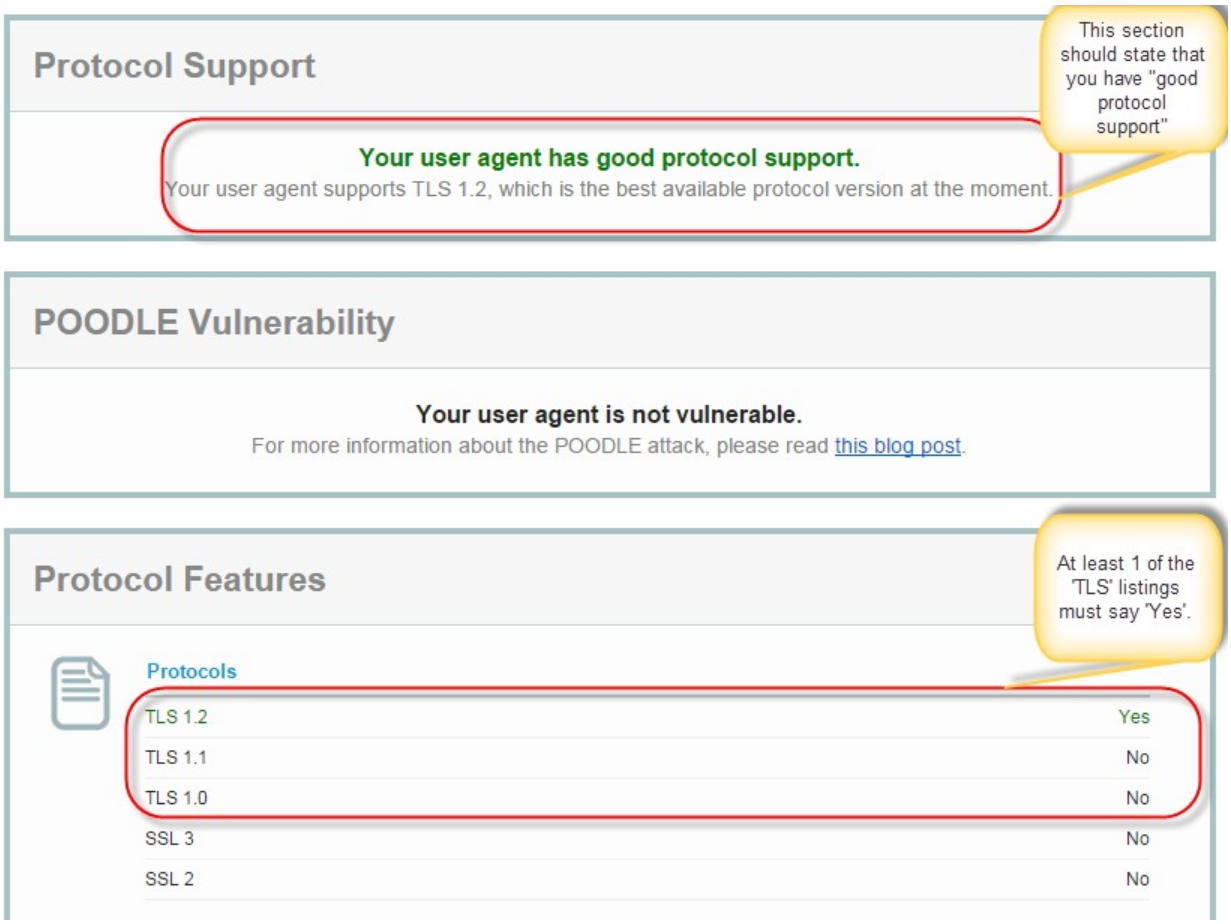
SUBJECT: **REMINDER - OCC DISABLING SSL 3.0 ENCRYPTION (POODLE)**

OCC places the trust and protection of our customers' data with a high regard and we want to ensure that we have the highest levels of security for our systems. We are committed to protecting the ability of our clients to access OCC's services and applications securely and with the integrity of the data you entrust with us.

On October 15, 2014 Google researchers published details on a security vulnerability (CVE-2014-3566) that affects the Secure Socket Layer (SSL) 3.0 encryption protocol, also known as "POODLE," which may allow a man-in-the-middle attack to extract data from secure HTTP connections. Although the vulnerability is somewhat difficult to exploit, to further protect customers, we will be disabling SSL 3.0 to fully address this issue.

OCC has worked diligently to identify those resources that could impact you and to implement our plan to address the Secure Socket Layer (SSLv3) internet vulnerability, POODLE. **On Saturday, March 14, 2015 we will permanently disable support for SSLv3 across all client facing web-based systems** accessed by OCC's clearing members and exchanges. In order to provide the highest levels of security OCC will be strictly supporting the Transport Layer Security (TLS) protocol. Any channels connecting to OCC web-based systems will need to use TLS 1.0 encryption or higher— TLS 1.0, 1.1, or 1.2, as of the date of this memo.

Prior to disabling SSLv3 for OCC production environments, OCC will be implementing this change in our external testing and training environments effective February 28, 2015 so we can assess our clients' connection to us in a solely TLS supported environment**.** If you are unsure if your systems support TLS, OCC recommends that you check SSL/TLS capabilities here and validate that the TLS protocols state "yes" and SSL protocols state "no" within the Protocol Features section (as shown below, or check with your internal IT department to confirm your firm's protocol.



Upon request, OCC can provide directions you can follow to activate TLS in your browsers if it is not already in place.

OCC apologizes for any inconvenience this may cause. If you have any questions regarding this memo, please contact Member Services Help Desk at the following numbers: 800-544-6091 or 800-621-6072. Within Canada, please call 800-424-7320. Clearing Members may also e-mail us at memberservices@theocc.com.