The Payment Card Industry Security Standards Council (PCI SSC) published a new version of the industry standard in April 2016. Version 3.2 noted several requirements as *Best Practices* (you may view the document here http://www.ewingoil.com/sites/ewingoil.com/files/PCI_DSS_v3-2.pdf). Effective February 1, 2018, these Best Practices will become *Requirements*.

Version 3.2 includes five new sub-requirements within the 12 core requirements for PCI DSS for service providers affecting requirements 3, 10, 11 and 12. New sub-requirements have also been added to requirement 8 to ensure multi-factor authentication is used for all non-console administrative access and all remote access in the cardholder environment. Additionally, there are two new appendices. (A summary of the changes may be found here http://www.ewingoil.com/sites/ewingoil.com/files/PCI_DSS_v3-2_Summary_of_Changes.pdf.)

The documentation supported in PCI DSS 3.2 include updated Self-Assessment Questionnaires, Attestation or Compliance forms, Report on Compliance templates, Frequently asked Questions and Glossary. All of these forms may be found on the PCI SSC website in the documents library (www.pcisecuritystandards.org).

The next PCI DSS deadline for disabling SSL/early TLS protocols to safeguard payment data will take place on July 1, 2018.