VISA BULLETIN

18 DECEMBER 2015

PCI SSC ANNOUNCES NEW MIGRATION DATES FOR SSL AND EARLY TLS

In April 2015, the PCI Security Standards Council (SSC) removed SSL and early TLS as an example of strong cryptography in PCI Data Security Standard (DSS) Version 3.1 and noted that the technologies can no longer be used after June 30, 2016. Payment system stakeholders from around the world expressed concerns that the implementation deadline was too aggressive, would significantly affect annual PCI DSS re-validation efforts and negatively impact business practices.

Visa worked with clients and stakeholders in every market to obtain feedback and coordinated with the PCI SSC to adjust the compliance requirements to include an extended timeframe for migration off of the old technology. The adjustments to the requirements are noted below:

- All processing and third party entities – including acquirers, processors, gateways and service providers – must provide a TLS 1.1 or greater service offering by June 2016.
- All new implementations must be enabled with TLS 1.1 or greater.
- All processing and third party entities must cutover to a secure version of TLS (as defined by NIST) effective June 2018 instead of June 2016.
- The use of SSL/TLS 1.0 within a POI terminal that can be verified as not being susceptible to all known exploits for SSL and early TLS, with no demonstrative risk, can be used beyond June 2018.

These dates provided by PCI SSC as of December 2015 supersede the original dates issued in both PCI DSS v3.1 and in the **Migrating from SSL and early TLS** Information Supplement in April 2015.

For more information and answers to questions about new timelines, requirements and reasons for the adjustments, please review these PCI SSC resources:

- **Bulletin**: Outlines details on the newly announced extension to implement a secure transition to TLS 1.1 or higher.
- **Webinar**: Features insights and practical guidance from the PCI SSC, the National Institute of Standards and Technology (NIST) and members of the assessment community on making this important transition to protect your data and your customers.
- **PCI SSC Information Supplement**: Provides guidance on use of interim risk mitigation approaches, migration recommendations and alternative options for strong cryptographic protocols.