DATA SECURITY ALERT

Security Best Practices

May 14, 2018

Data Security is top priority for DGN. We periodically publish Data Security Alerts regarding emergency security threats and best practices to help protect payment card data. Data Security Alerts may be useful by providing stakeholders with valuable information for mitigating security risks. Please provide this alert to your IT or Information Security Personnel.

SSL & Early TLS Migration

After June 30, 2018, all entities must have disabled all use of SSL/early TLS as a security control, in accordance with the PCI Data Security Standard (PCI DSS). For more information please refer to the PCI SSC's Information Supplement Migrating from SSL and Early TLS

Important points to keep in mind as the deadline approaches:

- All new implementations are to be based on TLS 1.1 or higher
- POI devices (and the termination points to which they connect) that can be verified as not being susceptible to any of the known exploits for SSL and early versions of TLS, may continue to use SSL /early TLS. However, those POIs (and their termination points) must have up-to-date patches, and only necessary extensions must be enabled. A formal Risk Mitigation and Migration Plan must also be maintained

Important Note: Discover Global Network will not "cut off" processing transactions even if you are unable to meet the deadline, or you are in compliance by the deadline but connect to downstream merchants who haven't converted on time, (i.e., there will be no enforcement of "rolling blackouts" or even "reject" services). However here are some actions you will need to take:

REQUIRED RESPONSE

- Except in the case of POIs as mentioned above, disable SSL and Early TLS entirely, and migrate to a more modern encryption protocol, and disable any fallback to both SSL and early TLS. *Entities are strongly encouraged to consider TLS v1.2*
- Verify compliance with PCI DSS. If SSL/Early TLS is used, the requirements in *PCI DSS Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS* must be completed. Contact your PCI Qualified Security Assessor (QSA) as soon as possible if you have any questions regarding your PCI compliance status
- Continue to support merchants that are not compliant, but segment them so that they do not affect the broader security and compliance of your environment

Refer to NIST SP 800-52 rev 1 for guidance, and the PCI SSC Webinar for clarifications and updates on secure TLS configurations.

If you have any questions about the contents of this alert, please contact the Discover Security Team DISCCompliance@Discover.com