Security Advisory:
PCI v3.1 Requirements-Changes to Encryption Protocols

Following the SSL/TLS vulnerabilities such as POODLE and BEAST, the National Institute of Standards and Technology (NIST) deems all encryption protocols before TLS 1.2 weak and insecure. Upgrading to a current, secure version of TLS is the only known way to remediate the inherent weakness in early TLS implementations. Accordingly, the PCI council has updated it's encryption protocol requirements.

BridgePay is dedicated to maintaining a high level of security and protecting its communications with our partners. As a result, BridgePay is taking a proactive approach to ensure we maintain the highest levels of security and compliance. As of **June 16, 2015,** BridgePay is fully supporting TLS 1.2 and Secure Hash Algorithm - SHA256. Over the course of the year, BridgePay will be migrating its systems to only support TLS 1.2 or greater. All systems connecting to BridgePay need to migrate off of TLS 1.0 and TLS 1.1 by **June 30, 2016**. After this date, only TLS 1.2 or greater will be supported.

What systems are affected?
Any system that makes an encrypted connection to BridgePay. This includes web browsers and terminals.

I connect with a web-browser. Am I affected?
Modern web-browsers such as Internet Explorer, FireFox and Chrome support TLS 1.2. Consult your IT department to ensure your system is configured correctly.

Who should I contact if my terminal needs to be upgraded to use TLS 1.2?
If your terminal does not support the TLS 1.2 protocol, contact your terminal provider for an upgrade.

PCI 3.1 Requirement Highlights:
PCI DSS 3.1 has updated requirements 2.2.3, 2.3 and 4.1 to remove SSL and early TLS as examples of strong cryptography:

- Effective immediately, new implementations must not use SSL or early TLS (1.0 or 1.1).
- SSL and early TLS cannot be used as security controls to protect payment data after 30 June 2016.

Below are some links that may help with understanding these changes:
PCI Security Standards - Migrating from SSL
PCI Security Standards - Summary of Changes
NIST Special Publication

Thank you,
Gateway Support
gateway.support@bridgepaynetwork.com