

**Date:** September 25, 2017

**To:** First Data Clients

**From:** First Data

**Platform:** North

**Status:** Initial Notification

**Regarding:** PCI Mandate for TLS Migration

In December 2015, the PCI Council released expanded guidance on the use of specific internet transmission protocols. The expanded guidance applies to publicly facing connections (via internet, VPN, or direct/dedicated) that store, process or transmit cardholder data at Acquirers, Processors, Gateways and Service Providers. The PCI Council has mandated that all public facing implementations of Secure Socket Layer (SSL) and early versions of Transport Layer Security (TLS 1.0) must be upgraded to a secure version of TLS (TLS 1.1 or greater) and that all insecure protocols be disabled by June 30, 2018.

In order to comply with these requirements and maintain the highest levels of data security, First Data updated our own standard to require the enablement of TLS 1.2 for applications by **February 15, 2018**. **After this date, First Data will no longer support non-compliant protocols (TLS 1.0 and earlier).**

**Because complying with the PCI Security Standard is a joint responsibility of First Data and our clients—and reducing the risk of non-compliance or disruption of service is of the utmost importance—First Data recommends all clients take the following actions:**

1. Validate their TLS connections with First Data
2. Ensure all existing applications that use TLS encryption protocols are enabled for TLS 1.2, before February 15, 2018. (First Data will continue to support TLS 1.1 on a limited basis however, we urge customers to connect using TLS 1.2 to ensure optimum security.)
3. Cease use of and disable SSL and TLS 1.0 as a security control for all interfaces, before February 15, 2018.

First Data appreciates your support during this industry-wide migration effort. The protection of our data and that of our clients is of paramount importance. Our team remains committed to ensuring First Data products and services are compliant with industry standards and PCI requirements.

Please direct any questions regarding the information about this initiative to your dedicated support channels.

*The information contained in this Alert is provided as a courtesy and is for general informational purposes only. This Alert is not intended to be a complete description of all applicable policies and procedures. The matters referenced in this Alert are subject to change without notice. Individual circumstances may vary. The information contained in this Alert may include, among other things, a compilation of documents received from third parties. First Data shall not be responsible for any inaccurate or incomplete information.*

*© 2017 First Data Corporation. All Rights Reserved. All trademarks, service marks and trade names referenced in this material are the property of their respective owners. This Alert may not be copied, reproduced or distributed in any manner whatsoever without the express written consent of First Data Corporation.*

The information in this message may be proprietary and/or confidential, and protected from disclosure. If the reader of this message is not the intended recipient, or an employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify First Data immediately by replying to this message and deleting it from your computer.