DTCC *Important Notice*

The Depository Trust & Clearing Corporation

Z #:	0215
Date:	May 14, 2020
To:	All Clients
From:	DTCC
Attention:	IT / Technology Operations & Information Security
Subject:	Client Connectivity Encryption

As part of our continuing efforts to provide the most robust and secure processing environments possible, DTCC will **end support** for any encryption protocols for browsers and API's that precede TLS v1.2 (Transport Layer Security) by **August 31st, 2020**[1] and for IBM MQ®, FTP (File Transfer Protocol), NDM (Network Data Mover) and unencrypted HTTP by **November 1st, 2020**.

This announcement by DTCC requires that all clients take the following actions as they relate to connectivity:

1. Upgrade to the **latest browser versions**[2] and upgrade to **Java v1.8** (If you connect via API) before August 31st 2020
2. Upgrade to **IBM MQ®** version 9.1 or later before November 1st 2020
3. Migrate from **FTP** to **sFTP** (Secure File Transfer Protocol) before November 1st 2020
4. Upgrade from **NDM** to **Connect:Direct Secure +** before November 1st 2020
5. Switch from unencrypted **HTTP** to encrypted **HTTPS** before November 1st 2020

Action number 1 above aligns with leading web browser developers Microsoft; Google; Apple; Mozilla who have all announced their intent to disable TLS 1.0 and 1.1 in the latest versions of their browsers in 2020.

DTCC is requiring that all clients take the actions above as soon as possible to reduce the risk of their connectivity with DTCC from being impacted and to reduce information security risks across the industry. For all questions or to confirm your compliance, please contact DTCC at SCCP@DTCC.COM.

[1] ***This date extension updates Important Notice Z0214 posted in November 2019***

[2] ***For more information related to DTCC browser standards and for links to upgrade, please visit www.dtcc.com/browsers.***

For more information on specific browser deprecation industry guidance, please see below:

Google

Google, for its part, plans to show deprecation warnings for the use of TLS 1.0 and 1.1 when it releases Chrome 72, and it'll disable those protocol versions with the release of Chrome 81. "This will affect users on early release channels starting **January 2020**," Google explained in an announcement.

Apple

The use of TLS versions 1.0 and 1.1 is down, with browser makers reporting that less than 1 percent of all connections are using those protocol versions. An Apple announcement indicated that "complete support [for those versions] will be removed from Safari in updates to Apple iOS and macOS beginning in **March 2020**."

Mozilla

Mozilla is planning to disable TLS 1.0 and 1.1 support in its Firefox browser "in **March of 2020**," according to an announcement, although this change likely will show up earlier in its pre-release browser versions. Mozilla's announcement suggested that while TLS 1.0 doesn't necessarily require immediate action, the protocol just lacks proper cryptographic capabilities. Mozilla recommends moving to TLS 1.3.

Microsoft

Microsoft announced plans to disable TLS 1.0 and 1.1 in its Edge and Internet Explorer 11 browsers "**in the first half of 2020**." The announcement added that "sites should begin to move off of TLS 1.0 and 1.1 as soon as is practical."