



Action Required:	<input checked="" type="checkbox"/> Review action items	<input checked="" type="checkbox"/> Notify internal teams	<input type="checkbox"/> Contact FIS™
-------------------------	---	---	---------------------------------------

Date: May 30, 2018

Distribution: Commercial Capture Xpress (CCX) Clients

Subject: *Action Required* - Commercial Capture Xpress (CCX) - Reminder - Production – Transport Layer Security (TLS) Change

Contact: If you have questions, open an FIS Client Portal ticket at <https://my.fisglobal.com/Login>. Login with your current credentials.

Description

You are receiving this notification because your financial institution utilizes Commercial Capture Xpress (CCX). At FIS™, our first priority is to protect the financial interactions of you and your customers. To achieve this, we apply a “Secure by Design” philosophy, whereby every action taken and every decision made is viewed through the lens of security. We have created a transition plan to migrate a secure version of the Transport Layer Security (TLS) encryption protocol that will be implemented and configured to reject fallback to Secure Sockets Layer (SSL) or early TLS.

Fifteen years ago, SSL v3.0 was superseded by TLS v1.0, which has since been superseded by TLS v1.1 and TLS v1.2. Early TLS no longer meets minimum security best practices or Payment Card Industry (PCI) compliance standards due to security vulnerabilities in the protocol. FIS has begun the transition to TLS v1.2 in advance of the PCI council mandated deadline of June 2018. Our transition encompasses removal of support for TLS v1.0 and disablement of all Cipher Block Chain (CBC) ciphers including Advanced Encryption Standard (AES)/Data Encryption Standard Cypher Block Chaining (DES CBC) by June of 2018.

Accordingly, FIS will enhance the CCX application to this security standard on Sunday, June 17, 2018. This will remove support of TLS 1.0 and 1.1. Clients will need to have TLS 1.2 enabled after June 17, 2018 in order to access the CCX application.

Client Action

Once FIS enhances the CCX application to the TLS 1.2 security standard on June 17, 2018, web browsers using the older TLS standards will be rejected. All clients using the CCX application MUST upgrade to a Web browser supporting the TLS 1.2 standard, or you may lose connectivity to the CCX application.

If you or your customers are using an older browser, you must update them prior to June 17, 2018, to avoid any possible loss of access to the CCX application. The following are the most current versions of the major browsers that support the TLS 1.2 security standard:

- Chrome 66
- Firefox 59
- Internet Explorer 11
- Safari 11
- Opera 52
- Edge 17

Due to the technical nature of the changes described in this communication, FIS recommends that a member of your organization’s technology staff and representatives of any third-party processor review this information.

FIS Action

FIS will deploy the security enhancement within the CCX application to remove support of TLS 1.0 and TLS 1.1, Sunday, June 17, 2018, during the standard maintenance window 12:00 AM – 06:00 AM CT.