



Important Notice
Fixed Income Clearing Corporation - MBS

B #:	MBS1437-25
Date:	April 15, 2025
To:	Mortgage-Backed Securities Participants and Members
Category:	Connectivity Security Requirements and Standards
From:	DTCC Chief Information Security Officer and President, Clearing and Securities Services
Attention:	Technology Risk Officers and Managers, Technical Connectivity Managers
Subject:	Deadline to Apply SFTP Encryption Standards – FICC MBS Secure Connections

The Secure File Transfer Protocol (SFTP) encryption requirements set forth at the bottom of this notice must be successfully implemented by MBS Members **no later than May 31, 2025** to avoid fines and service disruptions.

Compliance with DTCC Security and Encryption Standards is mandatory and, as stated in Important Notices dated [September 30, 2024](#) and [April 19, 2024](#), the use of SFTP with specified encryption is a requirement of MBS membership.

Members that have not complied with the SFTP encryption requirements by May 31, 2025 will be in violation of MBS Rule 3 Section 2, which states that each Member must maintain or upgrade their network technology within the time periods as provided by an Important Notice posted to DTCC's website. Such Members will be subject to a \$5000 fine.

In addition to being assessed a fine, for Members that have not voluntarily complied with the SFTP encryption requirements by May 31, FICC will disable access to the legacy encryption configuration and such Members will need to implement alternative, approved methods to continue to access and use MBS's services.

To avoid fines and service interruptions, it is imperative that Members **complete testing by May 1, 2025** and implement the required encryption standards by May 31, 2025. To ensure the successful completion of SFTP encryption reconfiguration testing, DTCC has scheduled two weekend test windows on April 19, 2025, and April 26, 2025, from 8:00 AM to 11:00 AM ET. During these windows, all non-compliant encryptions in the Mainframe will be temporarily removed to facilitate connectivity testing.

Members are encouraged to contact DTCC Connectivity, sccp@dtcc.com, to confirm and validate that the upgrade has been performed successfully **prior to the May 31, 2025** deadline.

DTCC offers enhanced access to all important notices via a Web-based subscription service. The notification system leverages RSS Newsfeeds, providing significant benefits including real-time updates and customizable delivery. To learn more and to set up your own DTCC RSS alerts, visit http://www.dtcc.com/subscription_form.php.

Action Required:

The following key exchange algorithms, ciphers, and MACs must be used:

Key Exchange Algorithms:

ecdh-sha2-nistp521
ecdh-sha2-nistp384
ecdh-sha2-nistp256
diffie-hellman-group18-sha512
diffie-hellman-group16-sha512
diffie-hellman-group14-sha256

Ciphers

aes256-ctr
aes256-cbc
aes192-ctr
aes192-cbc

MACs

hmac-sha2-512
hmac-sha2-256

Members must review whether the key exchange algorithms, ciphers, and MACs not listed can be disabled or removed. If disabling or removing is not possible, the next option is to reorder them. This is a Participant/Member-side change only, meaning DTCC servers will be upgraded to accept only the secure encryption key exchange algorithms, ciphers, and MACs listed above.