Required fields are shown with yellow backgrounds and asterisks.

Page 1 of * 52

SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549
Form 19b-4

File No. * SR 2022 - * 003
Amendment No. (req. for Amendments *)

Filing by Fixed Income Clearing Corporation

Pursuant to Rule 19b-4 under the Securities Exchange Act of 1934

Initial * ☑ Amendment * ☐ Withdrawal ☐

Section 19(b)(2) * ☑ Section 19(b)(3)(A) * ☐ Section 19(b)(3)(B) * ☐

Pilot ☐

Extension of Time Period for Commission Action * ☐

Date Expires *

Rule

☐ 19b-4(f)(1) ☐ 19b-4(f)(4)
☐ 19b-4(f)(2) ☐ 19b-4(f)(5)
☐ 19b-4(f)(3) ☐ 19b-4(f)(6)

Notice of proposed change pursuant to the Payment, Clearing, and Settlement Act of 2010

Section 806(e)(1) * ☐ Section 806(e)(2) * ☐

Security-Based Swap Submission pursuant to the Securities Exchange Act of 1934 Section 3C(b)(2) * ☐

Exhibit 2 Sent As Paper Document ☐

Exhibit 3 Sent As Paper Document ☐

Description

Provide a brief description of the action (limit 250 characters, required when Initial is checked *).

Require Applicants and Members to Maintain or Upgrade Their Network or Communications Technology

Contact Information

Provide the name, telephone number, and e-mail address of the person on the staff of the self-regulatory organization prepared to respond to questions and comments on the action.

First Name * [redacted] Last Name * [redacted]

Title * [redacted]

E-mail * RuleFilingAdmin@dtcc.com

Telephone * [redacted] Fax

Signature

Pursuant to the requirements of the Securities Exchange of 1934, Fixed Income Clearing Corporation has duty caused this filing to be signed on its behalf by the undersigned thereunto duty authorized.

Date 05/20/2022

By [redacted]
(Name *)

(Title *) [redacted]

NOTE: Clicking the signature block at right will initiate digitally signing the form. A digital signature is as legally binding as a physical signature, and once signed, this form cannot be changed.

Date: 2022.05.20 13:27:33 -04'00'

Required fields are shown with yellow backgrounds and astericks.

SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

For complete Form 19b-4 instructions please refer to the EFFS website.

Form 19b-4 Information *

Add | Remove | View

Narrative - FICC Tech Upgrade Rule (

The self-regulatory organization must provide all required information, presented in a clear and comprehensible manner, to enable the public to provide meaningful comment on the proposal and for the Commission to determine whether the proposal is consistent with the Act and applicable rules and regulations under the Act.

Exhibit 1 - Notice of Proposed Rule Change *

Add | Remove | View

Exhibit 1A - FICC Tech Upgrade Rule

The Notice section of this Form 19b-4 must comply with the guidelines for publication in the Federal Register as well as any requirements for electronic filing as published by the Commission (if applicable). The Office of the Federal Register (OFR) offers guidance on Federal Register publication requirements in the Federal Register Document Drafting Handbook, October 1998 Revision. For example, all references to the federal securities laws must include the corresponding cite to the United States Code in a footnote. All references to SEC rules must include the corresponding cite to the Code of Federal Regulations in a footnote. All references to Securities Exchange Act Releases must include the release number, release date, Federal Register cite, Federal Register date, and corresponding file number (e.g., SR-[SRO]-xx-xx). A material failure to comply with these guidelines will result in the proposed rule change being deemed not properly filed. See also Rule 0-3 under the Act (17 CFR 240.0-3)

Exhibit 1A - Notice of Proposed Rule Change, Security-Based Swap Submission, or Advanced Notice by Clearing Agencies *

Add | Remove | View

The Notice section of this Form 19b-4 must comply with the guidelines for publication in the Federal Register as well as any requirements for electronic filing as published by the Commission (if applicable). The Office of the Federal Register (OFR) offers guidance on Federal Register publication requirements in the Federal Register Document Drafting Handbook, October 1998 Revision. For example, all references to the federal securities laws must include the corresponding cite to the United States Code in a footnote. All references to SEC rules must include the corresponding cite to the Code of Federal Regulations in a footnote. All references to Securities Exchange Act Releases must include the release number, release date, Federal Register cite, Federal Register date, and corresponding file number (e.g., SR-[SRO]-xx-xx). A material failure to comply with these guidelines will result in the proposed rule change being deemed not properly filed. See also Rule 0-3 under the Act (17 CFR 240.0-3)

Exhibit 2- Notices, Written Comments, Transcripts, Other Communications

Add | Remove | View

Copies of notices, written comments, transcripts, other communications. If such documents cannot be filed electronically in accordance with Instruction F, they shall be filed in accordance with Instruction G.

☐ Exhibit Sent As Paper Document

Exhibit 3 - Form, Report, or Questionnaire

Add | Remove | View

Copies of any form, report, or questionnaire that the self-regulatory organization proposes to use to help implement or operate the proposed rule change, or that is referred to by the proposed rule change.

☐ Exhibit Sent As Paper Document

Exhibit 4 - Marked Copies

Add | Remove | View

The full text shall be marked, in any convenient manner, to indicate additions to and deletions from the immediately preceding filing. The purpose of Exhibit 4 is to permit the staff to identify immediately the changes made from the text of the rule with which it has been working.

Exhibit 5 - Proposed Rule Text

Add | Remove | View

Exhibit 5 - FICC Tech Upgrade Rule (F

The self-regulatory organization may choose to attach as Exhibit 5 proposed changes to rule text in place of providing it in Item I and which may otherwise be more easily readable if provided separately from Form 19b-4. Exhibit 5 shall be considered part of the proposed rule change

Partial Amendment

Add | Remove | View

If the self-regulatory organization is amending only part of the text of a lengthy proposed rule change, it may, with the Commission's permission, file only those portions of the text of the proposed rule change in which changes are being made if the filing (i.e. partial amendment) is clearly understandable on its face. Such partial amendment shall be clearly identified and marked to show deletions and additions.

1. Text of the Proposed Rule Change

(a) The proposed rule change of Fixed Income Clearing Corporation ("FICC") is annexed hereto as Exhibit 5 and consists of modifications to FICC's Government Securities Division ("GSD") Rulebook ("GSD Rules"), FICC's Mortgage-Backed Securities Division ("MBSD") Clearing Rules ("MBSD Rules"), and the Electronic Pool Notification ("EPN") Rules of MBSD ("EPN Rules," and, together with the GSD Rules and the MBSD Rules, the "Rules")[1] to revise certain provisions in the Rules relating to the requirement of applicants and Members, (collectively, "Participants") of FICC, to require that each Participant upgrade its network technology, and communications technology or protocols to meet standards that FICC shall publish from time to time. Each of the proposed changes are described in greater detail below.

(b) Not applicable.

(c) Not applicable.

2. Procedures of the Self-Regulatory Organization

The proposed rule change was approved by the Risk Committee of the FICC Board of Directors on December 14, 2021.

3. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

(a) Purpose

FICC is proposing to adopt a requirement that each Participant provide documentation demonstrating that the Participant's network technology, and communication technology or protocols meet the standards that FICC is currently requiring. The determination to require changes or upgrades is incorporated into FICC's procedures and includes an evaluation of the external threat landscape, threats to FICC's technology infrastructure and information assets, industry cybersecurity priorities, a review of the root causes of incidents, and an evaluation of the current state of the network infrastructure as expressed using third party assessments. For existing Participants, a new requirement is being proposed to require such Participants to upgrade their network technology, and communication technology or protocols within the timeframe published by FICC. The proposed changes are described in greater detail below.

---

[1] Capitalized terms not defined herein are defined in the Rules, available at http://www.dtcc.com/legal/rules-and-procedures. References to "Members" in this filing include the Participants of GSD and MBSD, including GSD Netting Members, GSD Comparison-Only Members, GSD Sponsoring Members, GSD CCIT Members, GSD Funds-Only Settling Bank Members, MBSD Clearing Members, MBSD Cash Settling Bank Members, and MBSD EPN Users, as such terms are defined in the respective Rules.

(i) Background of the Requirement

Currently, FICC does not require, either as part of its application for membership or as an ongoing membership requirement, any level or version for network technology, such as a web browser or other technology, or any level or version of communications technology or protocols, such as email encryption, secure messaging, or file transfers, that are being used to connect to or communicate with FICC. In the current environment, FICC maintains multiple network and communications methods and protocols, some either obsolete or many years older than the current standard in order to support Participants using these older technologies, which leaves communications between FICC and its Participants vulnerable to interception or the introduction of unknown entries, and requires FICC to expend additional resources, both in personnel and equipment, to maintain older communications channels. In addition, Participant's use of older technology delays the implementation by FICC to upgrade its internal systems, which, by doing so, risks losing connectivity with a number of Participants. Given FICC's critical role in the marketplace, this is a risk that needs to be addressed.

FICC believes that it should require current network technology, and current communication technology and protocol standards for Participants connecting to its network. For example, The National Institute of Standards and Technology or NIST[2] Special Publication 800-52 revision 2, specifies servers that support government-only applications shall be configured to use TLS[3] 1.2 and should be configured to use TLS 1.3 as well. These servers should not be configured to use TLS 1.1 and shall not use TLS 1.0, SSL 3.0, or SSL 2.0.[4] The Internet Engineer Task Force ("IETF")[5] formally deprecated TLS versions 1.0 and 1.1 in March of 2021, stating, "These versions lack support for current and recommended cryptographic algorithms and mechanisms, and various government and industry profiles of applications using TLS now mandate avoiding these old TLS versions. … Removing support for older versions from implementations reduces the attack surface, reduces opportunity for misconfiguration, and streamlines library and product maintenance."[6] TLS 1.0 (published in 1999) does not support many modern, strong cipher (encryption) suites and TLS 1.1 (published in 2006) is a security

---

2 The National Institute of Standards and Technology ("NIST") is part of the U.S. Department of Commerce.

3 Transport Layer Security ("TLS"), the successor of the now-deprecated Secure Sockets Layer ("SSL"), is a cryptographic protocol designed to provide communications security over a computer network.

4 A government-only application is an application where the intended users are exclusively government employees or contractors working on behalf of the government. The full NIST publication is available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

5 The Internet Engineering Task Force ("IETF") is an open standards organization, which develops and promotes voluntary Internet standards, in particular the technical standards that comprise the Internet protocol suite (TCP/IP).

6 https://datatracker.ietf.org/doc/rfc8996/

improvement over TLS 1.0 but still does not support certain stronger cipher or encryption suites.[7] Another communications technology, File Transfer Protocol ("FTP") is considered an insecure protocol, because it transfers user authentication data (username and password) and file data as plain-text (not encrypted) over the network. This makes it highly vulnerable to sniffing attacks that allow an attacker to collect usernames and passwords from the network and inject malware into downloads via FTP. Following the guidance from NIST and other standards organizations, the proposed change would require the use of TLS 1.2, Secure FTP ("SFTP"), along with other modern technology and communication standards and protocols to communication with Participants.

(ii) Proposed Rule Changes

GSD Rules

FICC is proposing to modify GSD Rules Rule 2A, Section 5, Rule 3, Section 2, and Rule 3B, Section 3(c)(ii) and insert a new Rule 3A, Section 2(b)(v), which would be changed to add the requirement that applicants for Comparison-Only Members, Netting Members, Sponsoring Members, and CCIT Members respectively, must confirm their network technology, and communications technology and protocols to be at the levels specified by FICC, as part of their application. Rule 3, Section 2, Rule 3A, Section 2(e), and Rule 3B, Section 5(b)(i) would be amended to add the requirement that each Participant type maintain or upgrade their network technology, or communications technology or protocols on the systems that connect to the Corporation to the version being required and within the time periods as provided through the Important Notice mechanism on the Corporation's website. The GSD Rules Fine Schedule would be updated to provide that any Participant who fails to perform the upgrade to their network technology, or communications technology or protocols and in the required timeframe would be subject to a monetary fine, as specified in the Rules.

Also, FICC is proposing to re-number Rule 3A, Section 2(e) through Section 2(h) to Section 2(f) through Section 2(i) due to the insertion of a new Section 2(e); Rule 3B, Section 3(c)(ii) to Section 3(c)(iii) due to the insertion of a new Section 3(c)(ii); and Rule 3B, Section 5(i) and Section 5(ii) to Section 5(ii) and Section 5(iii) due to the insertion of a new Section 5(i).

MBSD Rules

To implement the proposed changes described herein, FICC would revise Rule 2A, Section 2(a) which would be changed to add the requirement that applicants for Clearing Members must confirm their network technology, and communications technology and protocols to be at the levels specified by FICC, as part of their application. Rule 3, Section 2 would be amended to add the requirement that each Clearing Member to maintain or upgrade their network technology, or communications technology or protocols on the systems that connect to the Corporation to the version being required and within the time periods as provided through the Important Notice mechanism on the Corporation's website. In addition, Rule 3, Section 2 would also be updated to provide that any Participant who fails to perform the upgrade to their network technology, or communications technology or protocols and in the required timeframe would be

---

[7] Id.

subject to a monetary fine, as specified in the Rules. Rule 3A, Section (d)(i)(2) would be amended to add the requirement that each Cash Settling Bank Member to maintain or upgrade their network technology, or communications technology or protocols on the systems that connect to the Corporation to the version being required and within the time periods as provided through the Important Notice mechanism on the Corporation's website. The Schedule of Charges for both the Broker Account Group and the Dealer Account Group would be updated to provide that a Clearing Member or Cash Settling Bank Member who fails to perform the upgrade to their network technology, or communications technology or protocols and in the required timeframe would be subject to a monetary fine, as specified in the Rules.

Also, FICC is proposing to re-number Rule 3A, Section (d)(i)(2) to Section (d)(i)(3) due to the insertion of a new Section (d)(i)(2).

EPN Rules

FICC is proposing to revise EPN Rules Article III, Rule 1, Section 2(b) which would be changed to add the requirement that applicants for EPN Users must confirm their network technology, and communications technology and protocols to be at the levels specified by FICC, as part of their application. Article III, Rule 1, Section 3(f) would be amended to add the requirement that each EPN User to maintain or upgrade their network technology, or communications technology or protocols on the systems that connect to the Corporation to the version being required and within the time periods as provided through the Important Notice mechanism on the Corporation's website.

Also, FICC is proposing to re-number Article III Rule 1, Section 2(b) to Section 2(c) due to the insertion of a new Section 2(b) and Article III, Rule 1, Section 3(f) would be re-numbered to Section 3(g) due to the insertion of a new Section 3(f).

In addition, Article V, Rule 3, would be amended to add the requirement that a Participant who fails to perform the upgrade to their network technology, or communications technology or protocols and in the required timeframe may be subject to a monetary fine, as specified in the Rules.

(iii) ***Implementation Timeframe and Notification Requirements***

In order to provide Participants adequate time to complete a required network technology, or communications technology or protocol upgrade, the time for a Participant to complete a required upgrade shall be set forth in the form of a notice posted on FICC's website with the timeline determined for the due date of any upgrade. FICC maintains a security policy and control standards that include a review of industry, vendor and U.S. Government best practice guidelines and timelines for security reviews which are used to determine whether an upgrade may be required. Due dates for an upgrade shall be published on the website based on FICC's reasonable estimates of the complexity or potential cost of an upgrade, an estimate of potential licensing fees, an estimate of the resources that may be needed to support an upgrade, or the urgency to remediate published vulnerabilities.

Applicants for membership shall be required to test connectivity to FICC using the current network technology or communications technology or protocols with their application for membership upon the effective date of the proposal.

(b) Statutory Basis

FICC believes that the proposal is consistent with the requirements of the Securities Exchange Act of 1934 ("Act")[8] and the rules and regulations thereunder applicable to a registered clearing agency. In particular, FICC believes that the proposed rule changes is consistent with Section 17A(b)(3)(F) of the Act,[9] and Rules 17Ad-22(e)(17)(i) and (ii), (21), and (23),[10] promulgated under the Act as discussed below.

Section 17A(b)(3)(F)

Section 17A(b)(3)(F) of the Act[11] requires, in part, that the Rules be designed to promote the prompt and accurate clearance and settlement of securities transactions, to assure the safeguarding of securities and funds which are in the custody or control of FICC or for which it is responsible and to remove impediments to and perfect the mechanism of a national system for the prompt and accurate clearance and settlement of securities transactions.

FICC believes that the proposed rule change requiring Participants to meet FICC's standards for network technology, or communications technology or protocols is consistent with this provision of the Act. By conditioning an entity's application to FICC on its use of FICC's current network technology and communications technology or protocols, FICC should be better enabled to reduce the cyber risks of electronically connecting to entities by reducing the risks of communication interception. Accordingly, the proposed requirement would allow FICC to reduce both FICC's and its Participants exposure to interception or the introduction of malware while communicating between the entities. Intercepting communications or the introduction of malware or altered data could potentially compromise FICC's ability to promptly and accurately settle securities transactions and safeguard securities funds. The proposal is designed to mitigate those risks and thereby promote the prompt and accurate clearance and settlement of securities transactions, to assure the safeguarding of securities and funds which are in the custody or control of FICC or for which it is responsible and to remove impediments to and perfect the mechanism of a national system for the prompt and accurate clearance and settlement of securities transactions. Providing a clear and consistent standard at the current level of network and communication security and technology would allow Participants to better understand their obligations with respect to such technology and communication requirements and providing a

---

8 15 U.S.C. 78a et seq.

9 15 U.S.C. 78q-1(b)(3)(F).

10 17 CFR 240.17Ad-22(e)(17), (e)(21), (e)(23).

11 15 U.S.C. 78q-1(b)(3)(F).

uniform obligation for Participants with respect to such requirements. As such, FICC believes the proposed rule change is consistent with Section 17A(b)(3)(F) of the Act.[12]

17Ad 22(e)(21)(iv)

In addition, the proposed rule change is designed to be consistent with Rule 17Ad 22(e)(21)(iv) promulgated under the Act. Rule 17Ad-22(e)(21)(iv) requires FICC to, inter alia, establish, implement, maintain and enforce written policies and procedures reasonably designed to be efficient and effective in meeting the requirements of its Participants and the markets it serves with regard to the use of network technology and communication technologies or protocols. The proposed rule change would enhance FICC's security through the use of current network technology, or communication technology or protocols, and would allow FICC to reduce its and its Participants' exposure to interception or the introduction of malware while communicating between the entities. This would eliminate the current use of multiple generations of network technology and communications technology and protocols, including ones that NIST no longer permits for use on government systems due to their insecurity. The proposed rule would require, after appropriate notice to Participants, future network technology and communication or protocol upgrades as technology and threats evolve to maintain secure connectivity.

Therefore, by reviewing and updating the efficiency and effectiveness of Participants' use of network technology and communication technology or protocols and procedures, FICC believes the proposed change is consistent with the requirements of Rule 17Ad-22(e)(21)(iv), promulgated under the Act.

Rule 17Ad-22(e)(17)(i)

FICC believes the proposed change is designed to reduce the following risks: (1) the risk of the communications between FICC and its Participants being intercepted or introducing malware or other unknown harmful elements into FICC's network that could cause harm to FICC; (2) the risk that a cyberattack or other unknown harmful elements could be introduced from a Participant that could cause harm to other Participants.[13]

In addition, the proposed rule change is designed to be consistent with Rule 17Ad-22(e)(17)(i) promulgated under the Act,[14] which requires FICC to establish, implement, maintain and enforce written policies and procedures reasonably designed to manage the covered clearing agency's operational risks by identifying plausible sources of operational risk, both internal and external, and mitigating their impact through the use of appropriate systems, policies, procedures, and controls.

---

12 Id.

13 17 CFR 240.17Ad-22(e)(17).

14 17 CFR 240.17Ad-22(e)(17)(i).

The use of old, obsolete, or insecure network technology or communications technologies or protocols, including communications between FICC and its Participants that are unencrypted, allowing for potential interception or making the communication highly vulnerable to sniffing attacks that allow an attacker to collect usernames and passwords from the network and inject malware, are examples of plausible sources of operational risks that FICC seeks to reduce. By requiring all Participants, after appropriate notice, to upgrade their network technology or communications technology or protocols to current standards, FICC seeks to enhance the security of its systems and the communications between it and its Participants.

Because the proposed change would help identify and manage such operational risks, FICC believes that it is consistent with the requirements of Rule 17Ad-22(e)(17)(i), promulgated under the Act.[15]

Rule 17Ad 22(e)(17)(ii)

In addition, the proposed rule change is designed to be consistent with Rule 17Ad-22(e)(17)(ii) promulgated under the Act, which requires FICC to establish, implement, maintain and enforce written policies and procedures reasonably designed ensure that systems have a high degree of security, resiliency, operational reliability, and adequate, scalable capacity.[16]

The use of unencrypted network technology and communications technology or protocols can allow a third party to intercept messages, insert malware, or change the message content, often without the knowledge of either the sender or recipient of the messages or files. Requiring Participants to upgrade their network technology and communications technology or protocols to more modern and secure methods, may eliminate many of the earlier threats.

Therefore, by requiring Participants to upgrade their network technology or communications technology or protocols, FICC believes that the proposed change is consistent with the requirements of Rule 17Ad-22(e)(17)(ii), promulgated under the Act.[17]

Rule 17Ad-22(e)(22)

In addition, the proposed rule change is designed to be consistent with Rule 17Ad-22(e)(22) promulgated under the Act, which requires FICC to use, or at a minimum accommodate, relevant internationally accepted communication procedures and standards in order to facilitate efficient payment, clearing, and settlement.[18]

The requirement to use industry approved communications technology or protocols, including those that NIST specifies as acceptable for use in government systems is a cornerstone

---

15 Id.

16 17 CFR 240.17Ad-22(e)(17)(ii).

17 Id.

18 17 CFR 240.17Ad-22(e)(22).

of the changes being proposed by FICC. The use of older, obsolete, or insecure network technology or communications technology or protocols, including those specified to not be used by the IETF[19] represents a risk to efficient payment, clearing and settlement.

Therefore, by requiring Participants to upgrade their network technology or communications technology or protocols, FICC believes that the proposed change is consistent with the requirements of Rule 17Ad-22(e)(22), promulgated under the Act.[20]

Rule 17Ad-22(e)(23)

The proposed rule change is also designed to be consistent with Rule 17Ad 22(e)(23)(i), (ii) and (iv) promulgated under the Act, which requires FICC to publicly disclose all relevant rules and material procedures, provide sufficient information to enable Participants to identify and evaluate the risks, fees, potential monetary fines, and other material costs they incur by participating in the covered clearing agency, and to provide a comprehensive public disclosure that describes FICC's material rules, policies, and procedures regarding FICC's legal, governance, risk management and operating framework.[21]

Network technology, or communications technology or protocols that are being updated would be posted on the FICC website and Participants may subscribe to receive updates to such information as it occurs. This allows current or prospective Participants the ability to understand the risks and potential costs they may incur as a Participant, including the potential costs to upgrade its network technology or communications technology or protocols to the standards published by FICC.

Therefore, by providing Participants with public and readily available access to the required network technology, or communications technology or protocols, FICC believes that the proposed change is consistent with the requirements of Rule 17Ad-22(e)(23)(i)(ii) and (iv), promulgated under the Act.[22]

4. Self-Regulatory Organization's Statement on Burden on Competition

FICC does not believe the proposed change to require Participants to have, or to upgrade their network technology or communications technology or protocols would have any impact, or impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act.[23] Although the addition of the requirement to upgrade to current network technology or communications technology or protocols would be adding obligations on Participants with

---

19 https://datatracker.ietf.org/doc/rfc8996/

20 17 CFR 240.17Ad-22(e)(22).

21 17 CFR 240.17Ad-23(e)(i), (ii), and (iv).

22 Id.

23 15 U.S.C. 78q–1(b)(3)(I).

respect to how they communicate with FICC, such obligations would be reasonable because the requirements to protect client and customer data would allow FICC to reduce both its and its Participants' exposure to interception or the introduction of malware while communicating between the entities.

FICC believes that the proposed change described herein is necessary in furtherance of the purposes of Section 17A(b)(3)(F) of the Act,[24] and Rules 17Ad-22(e)(17), (e)(21), (e)(22), and (e)(23).[25] The proposed changes to require Participants to upgrade their network technology, and communications technology or protocols, will (i) allow FICC to protect it and its Participants and would promote the prompt and accurate clearance and settlement of securities consistent with the requirements of Section 17A(b)(3)(F) of the Act,[26] (ii) identify potential operational risks from the use of obsolete and insecure network technology and communications technology or protocols consistent with Rule 17Ad 22(e)(17)(i),[27] (iii) through the requirement of the use of current network technology and communications technology or protocols, ensure that systems have a high degree of security, resiliency, operational reliability, and adequate, scalable capacity, consistent with Rule 17Ad 22(e)(17)(ii),[28] and (iv) through the use of requiring relevant internationally accepted communication procedures and standards, facilitate efficient payment, clearing, and settlement, consistent with Rules 17Ad-22(e)(22).[29]

FICC believes that the proposed change described herein is appropriate in furtherance of the Act because the NIST standards and frameworks provides a common language and systematic methodology for managing cybersecurity risk. The IETF, initially supported by the U.S. Government,[30] develops the internet and other technical standards used in communications between devices, and together, these are two of the leading providers of standards used by organizations to protect data and interoperability. FICC maintains policies to review current risks and standards, incorporating input from industry, vendors, and the U.S. Government to determine best practice guidelines and timelines for security reviews.

Therefore, FICC does not believe that the proposed change would impose any burden on competition that is not necessary or appropriate in furtherance of the Act.[31]

---

24 15 U.S.C. 78q-1(b)(3)(F).

25 17 CFR 240.17Ad-22(e)(1), (e)(17), (e)(21), (e)(22) and (e)(23).

26 Id.

27 17Ad 22(e)(17)(i).

28 17Ad 22(e)(17)(ii).

29 Id.

30 https://www.internetsociety.org/internet/history-of-the-internet/ietf-internet-society/

31 15 U.S.C. 78q-1(b)(3)(I).

5. Self-Regulatory Organization's Statement on Comments on the Proposed Rule Change Received from Members, Participants, or Others

FICC has not received or solicited any written comments relating to this proposal. If any written comments are received, they will be publicly filed as an Exhibit 2 to this filing, as required by Form 19b-4 and the General Instructions thereto.

Persons submitting comments are cautioned that, according to Section IV (Solicitation of Comments) of the Exhibit 1A in the General Instructions to Form 19b-4, the SEC does not edit personal identifying information from comment submissions. Commenters should submit only information that they wish to make available publicly, including their name, email address, and any other identifying information.

All prospective commenters should follow the SEC's instructions on how to submit comments, available at https://www.sec.gov/regulatory-actions/how-to-submit-comments. General questions regarding the rule filing process or logistical questions regarding this filing should be directed to the Main Office of the SEC's Division of Trading and Markets at tradingandmarkets@sec.gov or 202-551-5777.

FICC reserves the right not to respond to any comments received.

6. Extension of Time Period for Commission Action

FICC does not consent to an extension of the time period specified in Section 19(b)(2) of the Act[32] for Securities and Exchange Commission ("Commission") action.

7. Basis for Summary Effectiveness Pursuant to Section 19(b)(3) or for Accelerated Effectiveness Pursuant to Section 19(b)(2)

(a) Not applicable.

(b) Not applicable.

(c) Not applicable.

(d) Not applicable.

8. Proposed Rule Change Based on Rules of Another Self-Regulatory Organization or of the Commission

While the proposal is not based on the rules of another self-regulatory organization or of the Commission, FICC's affiliates, DTC and NSCC, have each filed similar proposals concurrently with this filing to adopt comparable rule changes.

9. Security-Based Swap Submissions Filed Pursuant to Section 3C of the Act

---

[32] 15 U.S.C. 78s(b)(2).

Not applicable.

10. Advance Notice Filed Pursuant to Section 806(e) of the Payment, Clearing, and Settlement Supervision Act of 2010

Not applicable.

11. Exhibits

Exhibit 1 – Not applicable.

Exhibit 1A – Notice of proposed rule change for publication in the Federal Register.

Exhibit 2 – Not applicable.

Exhibit 3 – Not applicable.

Exhibit 4 – Not applicable.

Exhibit 5 – Proposed changes to the Rules.

EXHIBIT 1A

SECURITIES AND EXCHANGE COMMISSION
(Release No. 34-[_____]; File No. SR-FICC-2022-003)

[DATE]

Self-Regulatory Organizations; Fixed Income Clearing Corporation; Notice of Filing of a Proposed Rule Change to Require Applicants and Members to Maintain or Upgrade Their Network or Communications Technology

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 ("Act")[1] and Rule 19b-4 thereunder,[2] notice is hereby given that on May __, 2022, Fixed Income Clearing Corporation ("FICC") filed with the Securities and Exchange Commission ("Commission") the proposed rule change as described in Items I, II and III below, which Items have been prepared by the clearing agency. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

I. Clearing Agency's Statement of the Terms of Substance of the Proposed Rule Change

The proposed rule change of FICC consists of modifications to FICC's Government Securities Division ("GSD") Rulebook ("GSD Rules"), FICC's Mortgage-Backed Securities Division ("MBSD") Clearing Rules ("MBSD Rules"), and the Electronic Pool Notification ("EPN") Rules of MBSD ("EPN Rules," and, together with the GSD Rules and the MBSD Rules, the "Rules")[3] to revise certain provisions in the

---

1 15 U.S.C. 78s(b)(1).

2 17 CFR 240.19b-4.

3 Capitalized terms not defined herein are defined in the Rules, available at http://www.dtcc.com/legal/rules-and-procedures. References to "Members" in this filing include the Participants of GSD and MBSD, including GSD Netting Members, GSD Comparison-Only Members, GSD Sponsoring Members, GSD CCIT Members, GSD Funds-Only Settling Bank Members, MBSD Clearing

Rules relating to the requirement of applicants and Members, (collectively, "Participants") of FICC, to require that each Participant upgrade its network technology, and communications technology or protocols to meet standards that FICC shall publish from time to time, as described in greater detail below.

II. Clearing Agency's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

In its filing with the Commission, the clearing agency included statements concerning the purpose of and basis for the proposed rule change and discussed any comments it received on the proposed rule change. The text of these statements may be examined at the places specified in Item IV below. The clearing agency has prepared summaries, set forth in sections A, B, and C below, of the most significant aspects of such statements.

(A) Clearing Agency's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

1. Purpose

FICC is proposing to adopt a requirement that each Participant provide documentation demonstrating that the Participant's network technology, and communication technology or protocols meet the standards that FICC is currently requiring. The determination to require changes or upgrades is incorporated into FICC's procedures and includes an evaluation of the external threat landscape, threats to FICC's technology infrastructure and information assets, industry cybersecurity priorities, a review of the root causes of incidents, and an evaluation of the current state of the

---

Members, MBSD Cash Settling Bank Members, and MBSD EPN Users, as such terms are defined in the respective Rules.

network infrastructure as expressed using third party assessments. For existing Participants, a new requirement is being proposed to require such Participants to upgrade their network technology, and communication technology or protocols within the timeframe published by FICC. The proposed changes are described in greater detail below.

(i) Background of the Requirement

Currently, FICC does not require, either as part of its application for membership or as an ongoing membership requirement, any level or version for network technology, such as a web browser or other technology, or any level or version of communications technology or protocols, such as email encryption, secure messaging, or file transfers, that are being used to connect to or communicate with FICC. In the current environment, FICC maintains multiple network and communications methods and protocols, some either obsolete or many years older than the current standard in order to support Participants using these older technologies, which leaves communications between FICC and its Participants vulnerable to interception or the introduction of unknown entries, and requires FICC to expend additional resources, both in personnel and equipment, to maintain older communications channels. In addition, Participant's use of older technology delays the implementation by FICC to upgrade its internal systems, which, by doing so, risks losing connectivity with a number of Participants. Given FICC's critical role in the marketplace, this is a risk that needs to be addressed.

FICC believes that it should require current network technology, and current communication technology and protocol standards for Participants connecting to its

network. For example, The National Institute of Standards and Technology or NIST[4] Special Publication 800-52 revision 2, specifies servers that support government-only applications shall be configured to use TLS[5] 1.2 and should be configured to use TLS 1.3 as well. These servers should not be configured to use TLS 1.1 and shall not use TLS 1.0, SSL 3.0, or SSL 2.0.[6] The Internet Engineer Task Force ("IETF")[7] formally deprecated TLS versions 1.0 and 1.1 in March of 2021, stating, "These versions lack support for current and recommended cryptographic algorithms and mechanisms, and various government and industry profiles of applications using TLS now mandate avoiding these old TLS versions. … Removing support for older versions from implementations reduces the attack surface, reduces opportunity for misconfiguration, and streamlines library and product maintenance."[8] TLS 1.0 (published in 1999) does not support many modern, strong cipher (encryption) suites and TLS 1.1 (published in 2006) is a security improvement over TLS 1.0 but still does not support certain stronger

---

4 The National Institute of Standards and Technology ("NIST") is part of the U.S. Department of Commerce.

5 Transport Layer Security ("TLS"), the successor of the now-deprecated Secure Sockets Layer ("SSL"), is a cryptographic protocol designed to provide communications security over a computer network.

6 A government-only application is an application where the intended users are exclusively government employees or contractors working on behalf of the government. The full NIST publication is available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

7 The Internet Engineering Task Force ("IETF") is an open standards organization, which develops and promotes voluntary Internet standards, in particular the technical standards that comprise the Internet protocol suite (TCP/IP).

8 https://datatracker.ietf.org/doc/rfc8996/

cipher or encryption suites.[9] Another communications technology, File Transfer Protocol ("FTP") is considered an insecure protocol, because it transfers user authentication data (username and password) and file data as plain-text (not encrypted) over the network. This makes it highly vulnerable to sniffing attacks that allow an attacker to collect usernames and passwords from the network and inject malware into downloads via FTP. Following the guidance from NIST and other standards organizations, the proposed change would require the use of TLS 1.2, Secure FTP ("SFTP"), along with other modern technology and communication standards and protocols to communication with Participants.

(ii) Proposed Rule Changes

GSD Rules

FICC is proposing to modify GSD Rules Rule 2A, Section 5, Rule 3, Section 2, and Rule 3B, Section 3(c)(ii) and insert a new Rule 3A, Section 2(b)(v), which would be changed to add the requirement that applicants for Comparison-Only Members, Netting Members, Sponsoring Members, and CCIT Members respectively, must confirm their network technology, and communications technology and protocols to be at the levels specified by FICC, as part of their application. Rule 3, Section 2, Rule 3A, Section 2(e), and Rule 3B, Section 5(b)(i) would be amended to add the requirement that each Participant type maintain or upgrade their network technology, or communications technology or protocols on the systems that connect to the Corporation to the version being required and within the time periods as provided through the Important Notice mechanism on the Corporation's website. The GSD Rules Fine Schedule would be

---

9 Id.

updated to provide that any Participant who fails to perform the upgrade to their network technology, or communications technology or protocols and in the required timeframe would be subject to a monetary fine, as specified in the Rules.

Also, FICC is proposing to re-number Rule 3A, Section 2(e) through Section 2(h) to Section 2(f) through Section 2(i) due to the insertion of a new Section 2(e); Rule 3B, Section 3(c)(ii) to Section 3(c)(iii) due to the insertion of a new Section 3(c)(ii); and Rule 3B, Section 5(i) and Section 5(ii) to Section 5(ii) and Section 5(iii) due to the insertion of a new Section 5(i).

MBSD Rules

To implement the proposed changes described herein, FICC would revise Rule 2A, Section 2(a) which would be changed to add the requirement that applicants for Clearing Members must confirm their network technology, and communications technology and protocols to be at the levels specified by FICC, as part of their application. Rule 3, Section 2 would be amended to add the requirement that each Clearing Member to maintain or upgrade their network technology, or communications technology or protocols on the systems that connect to the Corporation to the version being required and within the time periods as provided through the Important Notice mechanism on the Corporation's website. In addition, Rule 3, Section 2 would also be updated to provide that any Participant who fails to perform the upgrade to their network technology, or communications technology or protocols and in the required timeframe would be subject to a monetary fine, as specified in the Rules. Rule 3A, Section (d)(i)(2) would be amended to add the requirement that each Cash Settling Bank Member to maintain or upgrade their network technology, or communications technology or

protocols on the systems that connect to the Corporation to the version being required and within the time periods as provided through the Important Notice mechanism on the Corporation's website. The Schedule of Charges for both the Broker Account Group and the Dealer Account Group would be updated to provide that a Clearing Member or Cash Settling Bank Member who fails to perform the upgrade to their network technology, or communications technology or protocols and in the required timeframe would be subject to a monetary fine, as specified in the Rules.

Also, FICC is proposing to re-number Rule 3A, Section (d)(i)(2) to Section (d)(i)(3) due to the insertion of a new Section (d)(i)(2).

EPN Rules

FICC is proposing to revise EPN Rules Article III, Rule 1, Section 2(b) which would be changed to add the requirement that applicants for EPN Users must confirm their network technology, and communications technology and protocols to be at the levels specified by FICC, as part of their application. Article III, Rule 1, Section 3(f) would be amended to add the requirement that each EPN User to maintain or upgrade their network technology, or communications technology or protocols on the systems that connect to the Corporation to the version being required and within the time periods as provided through the Important Notice mechanism on the Corporation's website.

Also, FICC is proposing to re-number Article III Rule 1, Section 2(b) to Section 2(c) due to the insertion of a new Section 2(b) and Article III, Rule 1, Section 3(f) would be re-numbered to Section 3(g) due to the insertion of a new Section 3(f).

In addition, Article V, Rule 3, would be amended to add the requirement that a Participant who fails to perform the upgrade to their network technology, or

communications technology or protocols and in the required timeframe may be subject to a monetary fine, as specified in the Rules.

(iii) ***Implementation Timeframe and Notification Requirements***

In order to provide Participants adequate time to complete a required network technology, or communications technology or protocol upgrade, the time for a Participant to complete a required upgrade shall be set forth in the form of a notice posted on FICC's website with the timeline determined for the due date of any upgrade. FICC maintains a security policy and control standards that include a review of industry, vendor and U.S. Government best practice guidelines and timelines for security reviews which are used to determine whether an upgrade may be required. Due dates for an upgrade shall be published on the website based on FICC's reasonable estimates of the complexity or potential cost of an upgrade, an estimate of potential licensing fees, an estimate of the resources that may be needed to support an upgrade, or the urgency to remediate published vulnerabilities.

Applicants for membership shall be required to test connectivity to FICC using the current network technology or communications technology or protocols with their application for membership upon the effective date of the proposal.

2. Statutory Basis

FICC believes that the proposal is consistent with the requirements of the Act[10] and the rules and regulations thereunder applicable to a registered clearing agency. In particular, FICC believes that the proposed rule changes is consistent with Section

---

10 15 U.S.C. 78a et seq.

17A(b)(3)(F) of the Act,[11] and Rules 17Ad-22(e)(17)(i) and (ii), (21), and (23),[12] promulgated under the Act as discussed below.

Section 17A(b)(3)(F)

Section 17A(b)(3)(F) of the Act[13] requires, in part, that the Rules be designed to promote the prompt and accurate clearance and settlement of securities transactions, to assure the safeguarding of securities and funds which are in the custody or control of FICC or for which it is responsible and to remove impediments to and perfect the mechanism of a national system for the prompt and accurate clearance and settlement of securities transactions.

FICC believes that the proposed rule change requiring Participants to meet FICC's standards for network technology, or communications technology or protocols is consistent with this provision of the Act. By conditioning an entity's application to FICC on its use of FICC's current network technology and communications technology or protocols, FICC should be better enabled to reduce the cyber risks of electronically connecting to entities by reducing the risks of communication interception. Accordingly, the proposed requirement would allow FICC to reduce both FICC's and its Participants exposure to interception or the introduction of malware while communicating between the entities. Intercepting communications or the introduction of malware or altered data could potentially compromise FICC's ability to promptly and accurately settle securities transactions and safeguard securities funds. The proposal is designed to mitigate those

---

11 15 U.S.C. 78q-1(b)(3)(F).

12 17 CFR 240.17Ad-22(e)(17), (e)(21), (e)(23).

13 15 U.S.C. 78q-1(b)(3)(F).

risks and thereby promote the prompt and accurate clearance and settlement of securities transactions, to assure the safeguarding of securities and funds which are in the custody or control of FICC or for which it is responsible and to remove impediments to and perfect the mechanism of a national system for the prompt and accurate clearance and settlement of securities transactions. Providing a clear and consistent standard at the current level of network and communication security and technology would allow Participants to better understand their obligations with respect to such technology and communication requirements and providing a uniform obligation for Participants with respect to such requirements. As such, FICC believes the proposed rule change is consistent with Section 17A(b)(3)(F) of the Act.[14]

17Ad 22(e)(21)(iv)

In addition, the proposed rule change is designed to be consistent with Rule 17Ad 22(e)(21)(iv) promulgated under the Act. Rule 17Ad-22(e)(21)(iv) requires FICC to, inter alia, establish, implement, maintain and enforce written policies and procedures reasonably designed to be efficient and effective in meeting the requirements of its Participants and the markets it serves with regard to the use of network technology and communication technologies or protocols. The proposed rule change would enhance FICC's security through the use of current network technology, or communication technology or protocols, and would allow FICC to reduce its and its Participants' exposure to interception or the introduction of malware while communicating between the entities. This would eliminate the current use of multiple generations of network technology and communications technology and protocols, including ones that NIST no

---

14 Id.

longer permits for use on government systems due to their insecurity. The proposed rule would require, after appropriate notice to Participants, future network technology and communication or protocol upgrades as technology and threats evolve to maintain secure connectivity.

Therefore, by reviewing and updating the efficiency and effectiveness of Participants' use of network technology and communication technology or protocols and procedures, FICC believes the proposed change is consistent with the requirements of Rule 17Ad-22(e)(21)(iv), promulgated under the Act.

Rule 17Ad-22(e)(17)(i)

FICC believes the proposed change is designed to reduce the following risks: (1) the risk of the communications between FICC and its Participants being intercepted or introducing malware or other unknown harmful elements into FICC's network that could cause harm to FICC; (2) the risk that a cyberattack or other unknown harmful elements could be introduced from a Participant that could cause harm to other Participants.[15]

In addition, the proposed rule change is designed to be consistent with Rule 17Ad-22(e)(17)(i) promulgated under the Act,[16] which requires FICC to establish, implement, maintain and enforce written policies and procedures reasonably designed to manage the covered clearing agency's operational risks by identifying plausible sources of operational risk, both internal and external, and mitigating their impact through the use of appropriate systems, policies, procedures, and controls.

---

15 17 CFR 240.17Ad-22(e)(17).

16 17 CFR 240.17Ad-22(e)(17)(i).

The use of old, obsolete, or insecure network technology or communications technologies or protocols, including communications between FICC and its Participants that are unencrypted, allowing for potential interception or making the communication highly vulnerable to sniffing attacks that allow an attacker to collect usernames and passwords from the network and inject malware, are examples of plausible sources of operational risks that FICC seeks to reduce. By requiring all Participants, after appropriate notice, to upgrade their network technology or communications technology or protocols to current standards, FICC seeks to enhance the security of its systems and the communications between it and its Participants.

Because the proposed change would help identify and manage such operational risks, FICC believes that it is consistent with the requirements of Rule 17Ad-22(e)(17)(i), promulgated under the Act.[17]

Rule 17Ad 22(e)(17)(ii)

In addition, the proposed rule change is designed to be consistent with Rule 17Ad-22(e)(17)(ii) promulgated under the Act, which requires FICC to establish, implement, maintain and enforce written policies and procedures reasonably designed ensure that systems have a high degree of security, resiliency, operational reliability, and adequate, scalable capacity.[18]

The use of unencrypted network technology and communications technology or protocols can allow a third party to intercept messages, insert malware, or change the message content, often without the knowledge of either the sender or recipient of the

---

17 Id.

18 17 CFR 240.17Ad-22(e)(17)(ii).

messages or files. Requiring Participants to upgrade their network technology and communications technology or protocols to more modern and secure methods, may eliminate many of the earlier threats.

Therefore, by requiring Participants to upgrade their network technology or communications technology or protocols, FICC believes that the proposed change is consistent with the requirements of Rule 17Ad-22(e)(17)(ii), promulgated under the Act.[19]

Rule 17Ad-22(e)(22)

In addition, the proposed rule change is designed to be consistent with Rule 17Ad-22(e)(22) promulgated under the Act, which requires FICC to use, or at a minimum accommodate, relevant internationally accepted communication procedures and standards in order to facilitate efficient payment, clearing, and settlement.[20]

The requirement to use industry approved communications technology or protocols, including those that NIST specifies as acceptable for use in government systems is a cornerstone of the changes being proposed by FICC. The use of older, obsolete, or insecure network technology or communications technology or protocols, including those specified to not be used by the IETF[21] represents a risk to efficient payment, clearing and settlement.

---

19 Id.

20 17 CFR 240.17Ad-22(e)(22).

21 https://datatracker.ietf.org/doc/rfc8996/

Therefore, by requiring Participants to upgrade their network technology or communications technology or protocols, FICC believes that the proposed change is consistent with the requirements of Rule 17Ad-22(e)(22), promulgated under the Act.[22]

Rule 17Ad-22(e)(23)

The proposed rule change is also designed to be consistent with Rule 17Ad 22(e)(23)(i), (ii) and (iv) promulgated under the Act, which requires FICC to publicly disclose all relevant rules and material procedures, provide sufficient information to enable Participants to identify and evaluate the risks, fees, potential monetary fines, and other material costs they incur by participating in the covered clearing agency, and to provide a comprehensive public disclosure that describes FICC's material rules, policies, and procedures regarding FICC's legal, governance, risk management and operating framework.[23]

Network technology, or communications technology or protocols that are being updated would be posted on the FICC website and Participants may subscribe to receive updates to such information as it occurs. This allows current or prospective Participants the ability to understand the risks and potential costs they may incur as a Participant, including the potential costs to upgrade its network technology or communications technology or protocols to the standards published by FICC.

Therefore, by providing Participants with public and readily available access to the required network technology, or communications technology or protocols, FICC

---

22 17 CFR 240.17Ad-22(e)(22).

23 17 CFR 240.17Ad-23(e)(i), (ii), and (iv).

believes that the proposed change is consistent with the requirements of Rule 17Ad-22(e)(23)(i)(ii) and (iv), promulgated under the Act.[24]

(B) Clearing Agency's Statement on Burden on Competition

FICC does not believe the proposed change to require Participants to have, or to upgrade their network technology or communications technology or protocols would have any impact, or impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act.[25] Although the addition of the requirement to upgrade to current network technology or communications technology or protocols would be adding obligations on Participants with respect to how they communicate with FICC, such obligations would be reasonable because the requirements to protect client and customer data would allow FICC to reduce both its and its Participants' exposure to interception or the introduction of malware while communicating between the entities.

FICC believes that the proposed change described herein is necessary in furtherance of the purposes of Section 17A(b)(3)(F) of the Act,[26] and Rules 17Ad-22(e)(17), (e)(21), (e)(22), and (e)(23).[27] The proposed changes to require Participants to upgrade their network technology, and communications technology or protocols, will (i) allow FICC to protect it and its Participants and would promote the prompt and accurate clearance and settlement of securities consistent with the requirements of Section

---

24 Id.

25 15 U.S.C. 78q–1(b)(3)(I).

26 15 U.S.C. 78q-1(b)(3)(F).

27 17 CFR 240.17Ad-22(e)(1), (e)(17), (e)(21), (e)(22) and (e)(23).

17A(b)(3)(F) of the Act,[28] (ii) identify potential operational risks from the use of obsolete and insecure network technology and communications technology or protocols consistent with Rule 17Ad 22(e)(17)(i),[29] (iii) through the requirement of the use of current network technology and communications technology or protocols, ensure that systems have a high degree of security, resiliency, operational reliability, and adequate, scalable capacity, consistent with Rule 17Ad 22(e)(17)(ii),[30] and (iv) through the use of requiring relevant internationally accepted communication procedures and standards, facilitate efficient payment, clearing, and settlement, consistent with Rules 17Ad-22(e)(22).[31]

FICC believes that the proposed change described herein is appropriate in furtherance of the Act because the NIST standards and frameworks provides a common language and systematic methodology for managing cybersecurity risk. The IETF, initially supported by the U.S. Government,[32] develops the internet and other technical standards used in communications between devices, and together, these are two of the leading providers of standards used by organizations to protect data and interoperability. FICC maintains policies to review current risks and standards, incorporating input from industry, vendors, and the U.S. Government to determine best practice guidelines and timelines for security reviews.

---

28 Id.

29 17Ad 22(e)(17)(i).

30 17Ad 22(e)(17)(ii).

31 Id.

32 https://www.internetsociety.org/internet/history-of-the-internet/ietf-internet-society/

Therefore, FICC does not believe that the proposed change would impose any burden on competition that is not necessary or appropriate in furtherance of the Act.[33]

(C) Clearing Agency's Statement on Comments on the Proposed Rule Change Received from Members, Participants, or Others

FICC has not received or solicited any written comments relating to this proposal. If any written comments are received, they will be publicly filed as an Exhibit 2 to this filing, as required by Form 19b-4 and the General Instructions thereto.

Persons submitting comments are cautioned that, according to Section IV (Solicitation of Comments) of the Exhibit 1A in the General Instructions to Form 19b-4, the SEC does not edit personal identifying information from comment submissions. Commenters should submit only information that they wish to make available publicly, including their name, email address, and any other identifying information.

All prospective commenters should follow the SEC's instructions on how to submit comments, available at https://www.sec.gov/regulatory-actions/how-to-submit-comments. General questions regarding the rule filing process or logistical questions regarding this filing should be directed to the Main Office of the SEC's Division of Trading and Markets at tradingandmarkets@sec.gov or 202-551-5777.

FICC reserves the right not to respond to any comments received.

III. Date of Effectiveness of the Proposed Rule Change, and Timing for Commission Action

Within 45 days of the date of publication of this notice in the Federal Register or within such longer period up to 90 days (i) as the Commission may designate if it finds

---

33 15 U.S.C. 78q-1(b)(3)(I).

such longer period to be appropriate and publishes its reasons for so finding or (ii) as to which the self-regulatory organization consents, the Commission will:

(A) by order approve or disapprove such proposed rule change, or

(B) institute proceedings to determine whether the proposed rule change should be disapproved.

IV. Solicitation of Comments

Interested persons are invited to submit written data, views and arguments concerning the foregoing, including whether the proposed rule change is consistent with the Act. Comments may be submitted by any of the following methods:

Electronic Comments:

- Use the Commission's Internet comment form (http://www.sec.gov/rules/sro.shtml); or
- Send an e-mail to rule-comments@sec.gov. Please include File Number SR-FICC-2022-003 on the subject line.

Paper Comments:

- Send paper comments in triplicate to Secretary, Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549.

All submissions should refer to File Number SR-FICC-2022-003. This file number should be included on the subject line if e-mail is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's Internet website (http://www.sec.gov/rules/sro.shtml). Copies of the submission, all subsequent amendments, all written statements with respect to the proposed rule change that are filed

with the Commission, and all written communications relating to the proposed rule change between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for website viewing and printing in the Commission's Public Reference Room, 100 F Street, NE, Washington, DC 20549 on official business days between the hours of 10:00 a.m. and 3:00 p.m. Copies of the filing also will be available for inspection and copying at the principal office of FICC and on DTCC's website (http://dtcc.com/legal/sec-rule-filings.aspx). All comments received will be posted without change. Persons submitting comments are cautioned that we do not redact or edit personal identifying information from comment submissions. You should submit only information that you wish to make available publicly. All submissions should refer to File Number SR-FICC-2022-003 and should be submitted on or before [insert date 21 days from publication in the Federal Register].

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.[34]

Secretary

---

34 17 CFR 200.30-3(a)(12).

EXHIBIT 5

Bold and underlined text indicates proposed added language

~~**Bold and strikethrough text**~~ indicates proposed deleted language

FIXED INCOME CLEARING CORPORATION

GOVERNMENT SECURITIES DIVISION RULEBOOK

RULE 2A – INITIAL MEMBERSHIP REQUIREMENTS

* * *

Section 5 – Application Documents

Each applicant to become a Member shall, as required by the Corporation from time to time, complete and deliver to the Corporation an Applicant Questionnaire in such form as may be prescribed by the Corporation. An applicant seeking membership in the Netting System shall also deliver to the Corporation the financial reports, other reports, opinions and other information as the Corporation determines appropriate.

Each applicant to become a Netting Member shall obtain and provide to the Corporation a Legal Entity Identifier.

As part of its membership application, each applicant (as determined by the Corporation with regard to membership type) shall complete and deliver to the Corporation (1) a FATCA Certification, and (2) a Cybersecurity Confirmation.

Each applicant must also have the successful completion of network and connectivity testing at the current FICC standards (the scope of such testing to be determined by the Corporation in its sole discretion).

* * *

RULE 3 – ONGOING MEMBERSHIP REQUIREMENTS

* * *

Section 2 - Reports by Netting Members

* * *

In addition to all of the above, each Member shall complete and deliver to the Corporation a Cybersecurity Confirmation at least every two years, on a date that is set by the Corporation and following notice that is provided no later than 180 calendar days prior to such due date.

In addition, each Member shall maintain or upgrade their network technology, or communications technology or protocols on the systems that connect to the Corporation to the version being required and within the time periods as provided by Important Notice posted to the Corporation's website.

* * *

RULE 3A—SPONSORING MEMBERS AND SPONSORED MEMBERS

* * *

Section 2 – Qualifications of Sponsoring Members, the Application Process and Continuance Standards

(a) A Netting Member shall be eligible to apply to become a Category 1 Sponsoring Member if: (i) it is a Bank Netting Member, (ii) it has a level of equity capital as of the end of the month prior to the effective date of its membership of at least $5 billion, (iii) it is "well-capitalized" as defined by the Federal Deposit Insurance Corporation's applicable regulations, and (iv) if it has a bank holding company that is registered under the Bank Holding Company Act of 1956, as amended, such bank holding company is also "well-capitalized" as defined by the applicable regulations of the Board of Governors of the Federal Reserve System. A Netting Member that is a Tier One Netting Member, other than an Inter-Dealer Broker Netting Member, or a Non-IDB Repo Broker with respect to activity in its Segregated Repo Account, shall be eligible to apply to become a Category 2 Sponsoring Member. The Corporation may require that a Person be a Netting Member for a time period deemed necessary by the Corporation before that Person may be considered to become a Sponsoring Member.

(b) (i) Each Netting Member applicant to become a Sponsoring Member shall complete and deliver to the Corporation an application in such form as may be prescribed by the Corporation from time to time and any other information requested by the Corporation. An application to become a Sponsoring Member shall first be reviewed by the Corporation. The Corporation shall recommend approval or disapproval of the application to the Board.

(ii) The Corporation may impose financial requirements on a Netting Member applying to become a Category 2 Sponsoring Member that are greater than financial requirements applicable to the applicant in its capacity as a Netting Member under Section 4(b) of Rule 2A, based upon the level of the anticipated positions and obligations of such applicant, the anticipated risk associated with the volume and types of transactions such applicant proposes to process through the Corporation as a Category 2 Sponsoring Member, and the overall financial condition of such applicant. The Board shall approve any increased financial requirements imposed by the Corporation in connection with the approval of an application of a Netting Member to become a Category 2 Sponsoring Member, and the Corporation shall thereafter regularly review such Category 2 Sponsoring Member regarding its compliance with such increased financial requirements.

(iii) If the Board denies the application of a Netting Member to become a Sponsoring Member, such denial shall be handled in the same way as set forth in Section 6 of Rule 2A with respect to membership applications.

(iv) Each Sponsoring Member, or any Netting Member applicant to become such, shall also furnish to the Corporation such adequate assurances of its financial responsibility and operational capability within the meaning of Section 7 of Rule 3 as the Corporation may at any time or from time to time deem necessary or advisable in order to

protect the Corporation and its members, to safeguard securities and funds in the custody or control of the Corporation and for which the Corporation is responsible, or to promote the prompt and accurate clearance and settlement of securities transactions. The Board shall approve any adequate assurances imposed by the Corporation in connection with the approval of an application of a Netting Member to become a Sponsoring Member, and the Corporation shall thereafter regularly review such Sponsoring Member regarding its compliance with such adequate assurances, as appropriate. Any adequate assurances imposed on a Sponsoring Member by the Corporation after its approval shall be communicated in writing to the Sponsoring Member, and the Corporation shall thereafter regularly review such Sponsoring Member regarding its compliance with such adequate assurances, as appropriate.

(v) Each Sponsoring Member or Netting Member applicant must also have the successful completion of network and connectivity testing at the current FICC standards (the scope of such testing to be determined by the Corporation in its sole discretion).

(c) Each Netting Member whose application is approved to become a Sponsoring Member shall sign and deliver to the Corporation a Sponsoring Member Agreement whereby the Netting Member shall agree to any terms and conditions deemed by the Corporation to be necessary in order to protect itself and its Members. Each Netting Member to become a Sponsoring Member shall also sign and deliver to the Corporation a Sponsoring Member Guaranty and a related legal opinion in a form satisfactory to the Corporation.

Nothing in these Rules shall prohibit a Sponsoring Member from seeking reimbursement from a Sponsored Member for payments made by the Sponsoring Member (whether pursuant to the Sponsoring Member Guaranty, out of Clearing Fund deposits or otherwise) with respect to obligations as to which the Sponsored Member is a principal obligor under these Rules, or as otherwise may be agreed by the Sponsored Member and Sponsoring Member.

(d) Each Sponsoring Member shall submit to the Corporation, within the timeframes and in the formats required by the Corporation, the reports and information that all Netting Members are required to submit regardless of type of Netting Member and the reports and information required to be submitted for its respective type of Netting Member, all pursuant to Section 2 of Rule 3. Each Sponsoring Member shall submit the Legal Entity Identifier for each of its Sponsored Member applicants as part of the application of such Sponsored Member applicant. Each Sponsoring Member shall provide the Corporation with a Legal Entity Identifier for each of its Sponsored Members such that the Corporation shall have a current Legal Entity Identifier for each Sponsored Member at all times. The Sponsoring Member shall indemnify the Corporation, and its employees, officers, directors, shareholders, agents, and Members (collectively, the "LEI Indemnified Parties"), for any and all losses, liabilities, expenses and Legal Actions suffered or incurred by the LEI Indemnified Parties arising from a Sponsoring Member's failure to have the current Legal Entity Identifiers of its Sponsored Members on file with the Corporation. "Legal Action" means and includes any claim, counterclaim, demand, action, suit, countersuit, arbitration, inquiry, proceeding or investigation before any federal, state or foreign court or other tribunal, or any investigative or regulatory agency or self-regulatory organization.

(e) Each Member shall maintain or upgrade their network technology, or communications technology or protocols on the systems that connect to the Corporation to the version being required and within the time periods as provided by Important Notice posted to the Corporation's website.

(**e**~~**f**~~) A Sponsoring Member's books and records, insofar as they relate to the Sponsored Member Trades submitted to the Corporation, shall be open to the inspection of the duly authorized representatives of the Corporation to the same extent provided in Section 10 of Rule 3 for other Members.

(~~**f**~~**g**) A Sponsoring Member shall promptly inform the Corporation, both orally and in writing, if it is no longer in compliance with the relevant standards and qualifications for applying to become a Sponsoring Member set forth in this Rule 3A. Notification must take place immediately and in no event later than 2 business days from the date on which the Sponsoring Member first learns of its non-compliance. The Corporation shall assess a $1,000 fine against any Sponsoring Member who fails to so notify the Corporation. If the Sponsoring Member fails to maintain a standard, the Corporation will, if necessary, undertake appropriate action to determine the status of the Sponsoring Member and its continued eligibility as such. In addition, the Corporation may review the financial responsibility and operational capability of the Sponsoring Member, and otherwise require from the Sponsoring Member additional reports of its financial or operational condition at such intervals and in such detail as the Corporation shall determine. In addition, if the Corporation has reason to believe that a Sponsoring Member may fail to comply with any of the Rules applicable to Sponsoring Members, it may require the Sponsoring Member to provide it, within such timeframe, and in such detail, and pursuant to such manner as the Corporation shall determine, with assurances in writing of a credible nature that the Sponsoring Member shall not, in fact, violate any of these Rules.

(**g**~~**h**~~) If a Category 1 Sponsoring Member falls below one or more of the required minimum financial standards for being a Sponsoring Member set forth in subsection (a) above, it shall, for the period beginning on the day on which it fell below such level and continuing until the later of the 90th calendar day after the date on which (i) it returned to compliance with such standard, or (ii) the Corporation received notice of the applicable violation, have a Sponsoring Member Omnibus Account Required Fund Deposit equal to the greater of either: (x) the sum of the normal calculation of its Sponsoring Member Omnibus Account Required Fund Deposit plus $1,000,000, or (y) 125 percent of the normal calculation of its Sponsoring Member Omnibus Account Required Fund Deposit. If, in the case of a Category 2 Sponsoring Member, the sum of the VaR Charges of its Sponsoring Member Omnibus Account(s) and its Netting System accounts exceeds its Netting Member Capital, the Category 2 Sponsoring Member shall not be permitted to submit activity into its Sponsoring Member Omnibus Account(s), unless otherwise determined by the Corporation in order to promote orderly settlement.

(~~**h**~~**i**) A Sponsoring Member may voluntarily elect to terminate its status as a Sponsoring Member, with respect to all Sponsored Members or with respect to one or more Sponsored Members from time to time, by providing the Corporation with a written notice of such termination ("Sponsoring Member Voluntary Termination Notice"). The Sponsoring Member shall specify in the Sponsoring Member Voluntary Termination Notice a desired date for the termination of the Sponsoring Member's status as such with respect to the Sponsored

Member(s) as to which the Sponsoring Member has terminated such status (the "Former Sponsored Members"), which date shall not be prior to the scheduled final settlement date of any remaining obligation owed by the Sponsoring Member with respect to the Former Sponsored Members to the Corporation as of the time such Sponsoring Member Voluntary Termination Notice is submitted to the Corporation, unless otherwise approved by the Corporation.

Such termination will not be effective until accepted by the Corporation, which shall be no later than 10 Business Days after the receipt of the Sponsoring Member Voluntary Termination Notice from such Sponsoring Member. The Corporation's acceptance shall be evidenced by a notice to all Members announcing the termination of the Sponsoring Member's status as such with respect to the Former Sponsored Members and the effective date of such termination (hereinafter the "Sponsoring Member Termination Date"). As of the Sponsoring Member Termination Date, the Sponsoring Member shall no longer be eligible to submit trades on behalf of its Former Sponsored Members and each of its Former Sponsored Members shall cease to be a Sponsored Member unless it is the Sponsored Member of another Sponsoring Member. If any trade is submitted to the Corporation by the Sponsoring Member on behalf of its Former Sponsored Members that is scheduled to settle on or after the Sponsoring Member Termination Date, such Sponsoring Member's Sponsoring Member Voluntary Termination Notice will be deemed void, and the Sponsoring Member will remain subject to this Rule as if it had not given such Sponsoring Member Voluntary Termination Notice.

A Sponsoring Member's voluntary termination of its status as such, in whole or in part, shall not affect its obligations to the Corporation, or the rights of the Corporation, including under the Sponsoring Member Guaranty, with respect to Sponsored Member Trades submitted to the Corporation before the applicable Sponsoring Member Termination Date. Any Sponsored Member Trades which have received the Corporation's guaranty of settlement and been novated to the Corporation shall continue to be processed and guaranteed by the Corporation.

(~~i~~**j**) Any non-public information furnished to the Corporation pursuant to this Rule shall be held in confidence as may be required under the laws, rules and regulations applicable to the Corporation that relate to the confidentiality of records. Each Sponsoring Member shall maintain DTCC Confidential Information in confidence to the same extent and using the same means it uses to protect its own confidential information, but no less than a reasonable standard of care and shall not use DTCC Confidential Information or disclose DTCC Confidential Information to any third party except as necessary to perform such Sponsoring Member's obligations under these Rules or as otherwise required by applicable law. Each Sponsoring Member acknowledges that a breach of its confidentiality obligations under these Rules may result in serious and irreparable harm to the Corporation and/or DTCC for which there is no adequate remedy at law. In the event of such a breach by the Sponsoring Member, the Corporation and/or DTCC shall be entitled to seek any temporary or permanent injunctive or other equitable relief in addition to any monetary damages hereunder.

* * *

RULE 3B – CENTRALLY CLEARED INSTITUTIONAL TRIPARTY SERVICE

* * *

Section 3 – Membership Application Process to Become a CCIT Member

(a) Each applicant to become a CCIT Member shall, as required by the Corporation from time to time, complete and deliver to the Corporation an Applicant Questionnaire in such form as may be prescribed by the Corporation and shall also deliver to the Corporation the financial reports, other reports, opinions and other information as the Corporation determines appropriate.

(b) Each applicant to become a CCIT Member or its Joint Account Submitter, as applicable, must also fulfill, within the timeframes established by the Corporation, any operational testing requirements (the scope of such testing to be determined by the Corporation in its sole discretion) and related reporting requirements (such as reporting the test results to the Corporation in a manner specified by the Corporation) that may be imposed by the Corporation to ensure the operational capability of the applicant.

(c) Each applicant shall complete and deliver to the Corporation:

(i) a FATCA Certification as part of its membership application. Without limiting the generality of the foregoing, if an applicant is a FFI Member, the Corporation shall require such applicant to certify and periodically to recertify to the Corporation that it is FATCA Compliant under such procedures as are set forth under FATCA, unless such requirements have been explicitly waived in writing by the Corporation; provided, however, that no such waiver will be issued if it shall cause the Corporation to be obligated to withhold under FATCA on gross proceeds from the sale or other disposition of any property. In addition, as part of its membership application, such applicant must agree that it shall indemnify the Corporation for any loss, liability or expense sustained by the Corporation as a result of its failing to be FATCA Compliant; ~~and~~

(ii) Each CCIT Member applicant must have the successful completion of network and connectivity testing at the current FICC standards (the scope of such testing to be determined by the Corporation in its sole discretion); and

(~~i~~**iii**) a Cybersecurity Confirmation.

* * *

Section 5 – On-going Membership Requirements

* * *

(b) Each CCIT Member shall submit to the Corporation the following:

(i) Each Member shall maintain or upgrade their network technology, or communications technology or protocols on the systems that connect to the

Corporation to the version being required and within the time periods as provided by Important Notice posted to the Corporation's website;

(~~i~~**ii**) disclosure on at least an annual basis regarding such CCIT Member's Net Assets, any financial statements the CCIT Member makes publicly available and such other reports, financial and other information as the Corporation from time to time may reasonably require. The time periods prescribed by the Corporation for such disclosure are set forth in the form of notices posted at the Corporation's website and/or distributed by the Corporation from time to time. It shall be the CCIT Member's responsibility to retrieve all notices daily from the Corporation's website; and

(~~ii~~**iii**) a completed Cybersecurity Confirmation at least every two years, on a date that is set by the Corporation and following notice that is provided no later than 180 calendar days prior to such due date.

* * *

FINE SCHEDULES

* * *

Failure to Maintain or Upgrade Network Technology, or Communications Technology or Protocols

Fine Name	Amount(s)
Failure to maintain or upgrade technology	**$5,000**

FIXED INCOME CLEARING CORPORATION

MORTGAGE-BACKED SECURITIES DIVISION

CLEARING RULES

RULE 2A – INITIAL MEMBERSHIP REQUIREMENTS

Section 1 - Eligibility for Membership: Clearing Members

Eligibility for Clearing Membership shall be as follows:

* * *

Section 2 - Membership Qualifications and Standards for Clearing Members

The Board may approve an application to become a Clearing Member by a Person that is eligible to apply to become a Clearing Member pursuant to this Rule upon a determination that such applicant meets the following requirements:

(a) Operational Capability - The applicant must be able to satisfactorily communicate with the Corporation, fulfill anticipated commitments to and meet the operational requirements of the Corporation with necessary promptness and accuracy, and conform to any condition and requirement that the Corporation reasonably deems necessary for its protection or that of its Members. The applicant agrees that it must fulfill, within the timeframes established by the Corporation, operational testing requirements (the scope of such testing to be determined by the Corporation in its sole discretion) and related reporting requirements (such as reporting test results to the Corporation in a manner specified by the Corporation) that may be imposed by the Corporation to ensure the continuing operational capability of the applicant. **Each applicant must have the successful completion of network and connectivity testing at the current FICC standards (the scope of such testing to be determined by the Corporation in its sole discretion).**

* * *

RULE 3 - ONGOING MEMBERSHIP REQUIREMENTS

* * *

Section 2 - Reports by Clearing Members

Each Clearing Member shall submit to the Corporation the reports and other information set forth below and such other reports and information as the Corporation from time to time may reasonably require. Unless specifically set forth below, the time periods prescribed by the Corporation are set forth in the form of notices posted at the Corporation's website and/or distributed by the Corporation from time to time. It shall be the Member's responsibility to retrieve all notices daily from the website.

* * *

In addition to all of the above, each Member shall complete and deliver to the Corporation a Cybersecurity Confirmation at least every two years, on a date that is set by the Corporation and following notice that is provided no later than 180 calendar days prior to such due date.

In addition, each Member shall maintain or upgrade their network technology, or communications technology or protocols on the systems that connect to the Corporation to the version being required and within the time periods as provided by Important Notice posted to the Corporation's website.

Notwithstanding anything to the contrary in this Rule, if a Member qualifies for more than one category of Clearing System membership, the Corporation, in its sole discretion, may require that such Member provide those reports and other financial or other information required to be provided to the Corporation by Members of any of those membership categories for which such Member qualifies.

All information provided to the Corporation shall be in English (and if translated into English, the translation must be a fair and accurate English translation).

A Member that fails to submit the above listed information **or upgrade their network technology, or communications technology or protocols on the systems that connect to the Corporation to the version being required** within the timeframes required by guidelines issued by the Corporation from time to time and in the manner requested, shall:

(i) be subject to a fine by the Corporation; and

(ii) until the required information is submitted to the Corporation, have a Clearing Fund deposit equal to the greater of either the sum of the normal calculation of its Required Fund Deposit plus $1,000,000, or 125 percent of the normal calculation of its Required Fund Deposit.

* * *

RULE 3A - CASH SETTLING BANK MEMBERS

* * *

(d) Each Cash Settling Bank Member:

(i) agrees:

(1) to abide by these Rules applicable to Cash Settling Bank Members and to be bound by all provisions thereof and that the Corporation shall have all the rights and remedies contemplated by the Rules; ~~**and**~~

(2) Each Cash Settling Bank Member shall maintain or upgrade their network technology, or communications technology or protocols on the systems that connect to the Corporation to the version being required and within the time periods as provided by Important Notice posted to the Corporation's website; and

(~~**2**~~**3**) to be bound by any amendment to these Rules with respect to any transaction occurring subsequent to such time such amendment takes effect as fully as though such amendment were now a part of these Rules.

* * *

FICC MORTGAGE-BACKED SECURITIES DIVISION
SCHEDULE OF CHARGES BROKER ACCOUNT GROUP

I. FEES

* * *

II. FINES

Failure to Maintain or Upgrade Network Technology, or Communications Technology or Protocols

Fine Name	Amount(s)
Failure to maintain or upgrade technology	$5,000

FICC MORTGAGE-BACKED SECURITIES DIVISION
SCHEDULE OF CHARGES DEALER ACCOUNT GROUP

I. FEES

* * *

II. FINES

Failure to Maintain or Upgrade Network Technology, or Communications Technology or Protocols

Fine Name	Amount(s)
Failure to maintain or upgrade technology	$5,000

FIXED INCOME CLEARING CORPORATION

MORTGAGE-BACKED SECURITIES DIVISION

EPN RULES

ARTICLE III
EPN USERS

Rule 1. Requirements Applicable to EPN Users

Sec. 1. Applicants Eligible to Become EPN Users

The Corporation shall provide services to those organizations, entities or persons who apply to the Corporation to become an EPN User, who qualify as an EPN User under these EPN Rules and whose EPN User Profiles are approved by the Corporation.

Sec. 2. Approval of Applicants

The Corporation shall approve an EPN User Profile, submitted by an applicant, to become an EPN User if the applicant:

(a) the applicant has affirmatively shown that it has the ability to satisfactorily communicate with the Corporation, fulfill anticipated commitments to and meet the operational requirements of the Corporation with necessary promptness and accuracy, and conform to any condition and requirement that the Corporation reasonably deems necessary for its protection or that of its Participants. The applicant agrees that it must fulfill, within the timeframes established by the Corporation, operational testing requirements (the scope of such testing to be determined by the Corporation in its sole discretion) and related reporting requirements (such as reporting test results to the Corporation in a manner specified by the Corporation) that may be imposed by the Corporation to ensure the continuing operational capability of the applicant; ~~**and**~~

(b) Each applicant must have the successful completion of network and connectivity testing at the current FICC standards (the scope of such testing to be determined by the Corporation in its sole discretion); and

(~~**b**~~**c**) has completed and delivered to the Corporation a Cybersecurity Confirmation.

* * *

Sec. 3. Agreements of EPN Users

An EPN User agrees :

(a) that the only service or system offered by the Corporation that it will utilize as an EPN User is the EPN Service;

(b) that, except to the extent waived by the Corporation, the EPN User shall abide by these EPN Rules and shall be bound by all the provisions thereof, and that the Corporation shall have all of the rights and remedies contemplated by these EPN Rules;

(c) that, except to the extent waived by the Corporation, these EPN Rules shall be a part of the terms and conditions of every contract or Message which the EPN User may make or have with the Corporation and of every contract or Message into which the EPN User, may enter which relates to the EPN Service;

(d) that, upon becoming an EPN User, the applicant shall utilize the EPN Service for all Messages relating to EPN Eligible Securities, except for those Messages which the Corporation specifically exempts and those Messages which both parties agree not to send through the EPN Service.

(e) that the EPN User shall pay to the Corporation (i) the compensation specified in the fee schedules of the Corporation for services rendered to the EPN User, (ii) such fines as may be imposed in accordance with these EPN Rules for the failure of the EPN User, to comply therewith, and (iii) such other amounts as may become payable to the Corporation by the EPN User, under these EPN Rules; ~~**and**~~

(f) addition, each Member shall maintain or upgrade their network technology, or communications technology or protocols on the systems that connect to the Corporation to the version being required and within the time periods as provided by Important Notice posted to the Corporation's website; and

(~~**f**~~**g**) that the EPN User shall be bound by any amendment to these EPN Rules with respect to any Message occurring subsequent to the time such amendment takes effect as fully as though such amendment were a part of these EPN Rules; provided, however, that no such amendment shall affect the EPN User's right to cease to be an EPN User.

* * *

ARTICLE V
MISCELLANEOUS

* * *

Rule 3. Fines and Other Sanctions

The Corporation may impose a fine on an EPN User for a violation of the EPN Rules or any order pursuant thereto or any agreement between the Corporation and the EPN User; for errors, delays or other conduct embarrassing the operations of the Corporation; or for not providing adequate facilities for its Messages with the Corporation or timely meeting its financial obligations to the Corporation. Fines imposed upon EPN Users for similar conduct occurring with similar frequency shall be uniform. **Each EPN User that fails to submit the above listed information or upgrade their network technology, or communications technology or protocols on the systems that connect to the Corporation to the version being required within the timeframes required by guidelines issued by the Corporation from time to time and in the manner requested, may be subject to a fine as provided in this section.**

* * *