OMB APPROVAL
OMB Number: 3235-0045 Estimated average burden hours per response.....38

Required fields are shown with yellow backgrounds and asterisks.

Page 1 of * 51

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

File No.* SR - 2019 - * 005
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)(2)
- ☐ 19b-4(f)(3)
- ☐ 19b-4(f)(4)
- ☐ 19b-4(f)(5)
- ☐ 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 Confirmation of Cybersecurity Program

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 * Allen Last Name * Brandt

Title * Executive Director and Associate General Counsel

E-mail * abrandt@dtcc.com

Telephone * (212) 855-5063 Fax

Signature

Pursuant to the requirements of the Securities Exchange Act of 1934,

has duly caused this filing to be signed on its behalf by the undersigned thereunto duly authorized.

Date 10/14/2019

By Nikki Poulos

(Name *)

(Title *)

Managing Director and Deputy General Counsel

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

npoulos@dtcc.com

Required fields are shown with yellow backgrounds and asterisks.

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

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

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 Advance 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, security-based swap submission, or advance notice 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

Exhibit Sent As Paper Document ☐

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 3 - Form, Report, or Questionnaire

Add Remove View

Exhibit Sent As Paper Document ☐

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 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

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] in order to (1) define "Cybersecurity Confirmation" as a signed, written representation that addresses the submitting firm's cybersecurity program; and (2) enhance the GSD and MBSD application requirements and ongoing requirements for Members to (a) require that a Cybersecurity Confirmation be provided as part of the application materials for all Members, and (b) require that all Members deliver to FICC a complete, updated Cybersecurity Confirmation at least every two years, as 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 Board of Directors of FICC at a meeting duly called and held on December 19, 2017.

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

(a) Purpose

(i) *Overview*

FICC is proposing to modify the Rules in order to (1) define "Cybersecurity Confirmation" as a signed, written representation that addresses the submitting firm's cybersecurity program; and (2) enhance the GSD and MBSD application requirements and ongoing requirements for Members to (a) require that a Cybersecurity Confirmation be provided as part of the application materials for all Members, and (b) require that all Members deliver to FICC a complete, updated Cybersecurity Confirmation at least every two years.

---

[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.

The proposed change would require all Members and applicants to deliver to FICC a signed, written Cybersecurity Confirmation, which includes representations regarding the submitting firm's cybersecurity program and framework. The Cybersecurity Confirmation would be required to be (1) delivered with the application materials for every applicant, and (2) updated and re-delivered at least every two years by all Members.

As described in more detail below, the Cybersecurity Confirmation would help FICC to assess the cybersecurity risks that may be introduced to it by Members that connect to FICC either through the Securely Managed and Reliable Technology ("SMART") network[2] or through other connections. The proposed Cybersecurity Confirmation would allow FICC to better understand its Members' cybersecurity programs and frameworks and identify possible cybersecurity risk exposures. Based on this information, FICC would be able to establish appropriate controls to mitigate these risks and their possible impacts to FICC's operations.

(ii) *Background of Proposal*

FICC believes it is prudent to better understand the cybersecurity risks that it may face through its interconnections to Members. As a designated systemically important financial market utility, or "SIFMU," FICC occupies a unique position in the marketplace such that a failure or a disruption to FICC could increase the risk of significant liquidity problems spreading among financial institutions or markets and thereby threaten the stability of the financial system in the United States.[3] Given its designation as a SIFMU, FICC believes it is prudent to develop an enhanced endpoint security framework designed so that its SMART network or other connectivity is adequately protected against cyberattacks.

Currently, FICC does not obtain any information regarding the security of a firm's systems or cybersecurity program prior to permitting that firm to connect either directly to the SMART network or to FICC through another means, such as through a third party service provider, service bureau, network, or the Internet. Given FICC's critical role in the marketplace, FICC is proposing to address the risks that could be posed by these connections.

---

2 The SMART network is a technology managed by FICC's parent company, The Depository Trust & Clearing Corporation ("DTCC"), that connects a nationwide complex of networks, processing centers and control facilities. This network extends between FICC's and its Members' operating premises. DTCC operates on a shared services model with respect to FICC and DTCC's other subsidiaries pursuant to intercompany agreements under which it is generally DTCC that provides a relevant service to its subsidiaries, including FICC.

3 FICC and its affiliates, The Depository Trust Company ("DTC") and National Securities Clearing Corporation ("NSCC"), were designated SIFMUs under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010. 12 U.S.C. 5465(e)(1).

Members may currently be subject to regulations that are designed, in part, to enhance the safeguards used by these entities to protect themselves against cyberattacks.[4] In order to comply with such regulations, Members and applicants would be required to follow standards established by national or international organizations focused on information security management, and would have already established protocols to allow their senior management to verify that they have sufficient cybersecurity programs in place to fulfill existing regulatory obligations. Other Members have established and follow substantially similar protocols because of evolving expectations by regulators or by institutional customers as to the sufficiency of their cyber safeguards. FICC believes that it should require confirmation of the cybersecurity standards utilized by its Members and applicants that connect to its network.

The proposed Cybersecurity Confirmation would require Members and applicants to represent that they have established adequate controls and security to help limit (1) cybersecurity risks to FICC and to the other Members' networks and (2) access by unauthorized third parties while the firm is connected to FICC either directly through the SMART network or through other connectivity such as a service provider, service bureau, network, or the Internet.

(iii) *Proposed Rule Changes*

FICC is proposing to modify its Rules to (1) define "Cybersecurity Confirmation;" and (2) require that firms deliver a completed Cybersecurity Confirmation (a) as part of their initial application with FICC, and (b) on an ongoing basis, at least every two years. Each of these proposed rule changes is described in greater detail below.

(1) *Proposed Cybersecurity Confirmation*

FICC is proposing to adopt a definition of "Cybersecurity Confirmation." Each Cybersecurity Confirmation would be required to be in writing on a form provided by FICC and signed by a designated senior executive of the submitting firm who is authorized to attest to these matters. Based on the form provided by FICC, each Cybersecurity Confirmation would contain representations regarding the submitting firm's cybersecurity program and framework. Such

---

[4] For example, depending on the type of entity, Members may be subject to one or more of the following regulations: (1) Regulation S-ID, which requires "financial institutions" or "creditors" under the rule to adopt programs to identify and address the risk of identity theft of individuals (17 CFR 248.201 - 202); (2) Regulation S-P, which requires broker-dealers, investment companies, and investment advisers to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information (17 CFR 248.1 - 30); and (3) Rule 15c3-5 under the Securities Exchange Act of 1934 ("Act"), known as the "Market Access Rule," which requires broker-dealers to establish, document, and maintain a system for regularly reviewing the effectiveness of its management controls and supervisory procedures (17 CFR 240.15c3-5).

representations by the submitting firm would cover the two years prior to the date of the most recently provided Cybersecurity Confirmation.

FICC is proposing to require that the following representations be included in the form of Cybersecurity Confirmation:

First, the Cybersecurity Confirmation would include a representation that the submitting firm has defined and maintains a comprehensive cybersecurity program and framework that considers potential cyber threats that impact the organization and protects the confidentiality, integrity and availability requirements of its systems and information.

Second, the Cybersecurity Confirmation would include a representation that the submitting firm has implemented and maintains a written enterprise cybersecurity policy or policies approved by the submitting firm's senior management or board of directors, and the organization's cybersecurity framework is in alignment with standard industry best practices and guidelines.[5]

Third, the Cybersecurity Confirmation would include a representation that, if the submitting firm is using a third party service provider or service bureau(s) to connect or transact business or to manage the connection with FICC, the submitting firm has an appropriate program to (a) evaluate the cyber risks and impact of these third parties, and (b) review the third party assurance reports.

Fourth, the Cybersecurity Confirmation would include a representation that the submitting firm's cybersecurity program and framework protect the segment of their system that connects to and/or interacts with FICC.

Fifth, the Cybersecurity Confirmation would include a representation that the submitting firm has in place an established process to remediate cyber issues identified to fulfill the submitting firm's regulatory and/or statutory requirements.

Sixth, the Cybersecurity Confirmation would include a representation that the submitting firm's cybersecurity program's and framework's risk processes are updated periodically based

---

[5] Examples of recognized frameworks, guidelines and standards that FICC believes are adequate include the Financial Services Sector Coordinating Council Cybersecurity Profile, the National Institute of Standards and Technology Cybersecurity Framework ("NIST CSF"), International Organization for Standardization ("ISO") standard 27001/27002 ("ISO 27001"), Federal Financial Institutions Examination Council ("FFIEC") Cybersecurity Assessment Tool, Critical Security Controls Top 20, and Control Objectives for Information and Related Technologies. FICC would identify recognized frameworks, guidelines and standards in the form of Cybersecurity Confirmation and in an Important Notice that FICC would issue from time to time. FICC would also consider accepting other standards upon request by a Member or applicant.

on a risk assessment or changes to technology, business, threat ecosystem, and/or regulatory environment.

And, finally, the Cybersecurity Confirmation would include a representation that the review of the submitting firm's cybersecurity program and framework has been conducted by one of the following: (1) the submitting firm, if it has filed and maintains a current Certification of Compliance with the Superintendent of the New York State Department of Financial Services confirming compliance with its Cybersecurity Requirements for Financial Services Companies;[6] (2) a regulator who assesses the program against an industry cybersecurity framework or industry standard, including those that are listed on the form of Cybersecurity Confirmation and in an Important Notice that is issued by FICC from time to time;[7] (3) an independent external entity with cybersecurity domain expertise in relevant industry standards and practices, including those that are listed on the form of Cybersecurity Confirmation and in an Important Notice that is issued by FICC from time to time;[8] or (4) an independent internal audit function reporting directly to the submitting firm's board of directors or designated board of directors committee, such that the findings of that review are shared with these governance bodies.

Together, the required representations are designed to provide FICC with evidence of each Member's or applicant's management of cybersecurity with respect to their connectivity to FICC. By requiring these representations from Members and applicants, the proposed Cybersecurity Confirmation would provide FICC with information that it could use to make decisions about risks or threats, perform additional monitoring, target potential vulnerabilities, and protect the FICC network.

---

6 23 N.Y. Comp. Codes R. & Regs. tit. 23, § 500 (2017). This regulation requires firms to confirm that they have a comprehensive cybersecurity program, as described in the regulation, which FICC believes is sufficient to meet the objectives of the proposed Cybersecurity Confirmation.

7 Industry cybersecurity frameworks and industry standards could include, for example, the Office of the Comptroller of the Currency or the FFIEC Cybersecurity Assessment Tool. FICC would identify acceptable industry cybersecurity frameworks and standards in the form of Cybersecurity Confirmation and in an Important Notice that FICC would issue from time to time. FICC would also consider accepting other industry cybersecurity frameworks and standards upon request by a Member or applicant.

8 A third party with cybersecurity domain expertise is one that follows and understands industry standards, practices and regulations that are relevant to the financial sector. Examples of such standards and practices include ISO 27001 certification or NIST CSF assessment. FICC would identify acceptable industry standards and practices in the form of Cybersecurity Confirmation and in an Important Notice that FICC would issue from time to time. FICC would also consider accepting other industry standards and practices upon request by a Member or applicant.

FICC is proposing to amend Rule 1 (Definitions) of the GSD Rules, Rule 1 (Definitions) of the MBSD Rules, and Rule 1 (Definitions) of Article I (Definitions and General Provisions) of the EPN Rules, to include a definition of "Cybersecurity Confirmation" as described above.

(2) *Initial and Ongoing Membership Requirement*

FICC is proposing to require that a Cybersecurity Confirmation be submitted to FICC by any applicant, as part of their application materials, and at least every two years by all Members. With respect to the requirement to deliver a Cybersecurity Confirmation at least every two years, FICC would provide all Members with notice of the date on which such Cybersecurity Confirmations would be due no later than 180 calendar days prior to such due date.

In order to implement these proposed changes, FICC would amend Section 5 of Rule 2A (Initial Membership Requirements) of the GSD Rules, Section 3 of Rule 3B (Centrally Cleared Institutional Triparty Service) of the GSD Rules, Section 4 of Rule 13 (Funds-Only Settlement) of the GSD Rules, Section 3 of Rule 2A (Initial Membership Requirements) of the MBSD Rules, Rule 3A (Cash Settlement Bank Members) of the MBSD Rules, and Section 2 of Rule 1 (Requirements Applicable to EPN Users) of Article III of the EPN Rules to require that applicants complete and deliver a Cybersecurity Confirmation as part of their application materials.

Further, FICC would amend Section 2 of Rule 3 (Ongoing Membership Requirements) of the GSD Rules, Section 5 of Rule 3B (Centrally Cleared Institutional Triparty Service) of the GSD Rules, Section 4 of Rule 13 (Funds-Only Settlement) of the GSD Rules, Section 2 of Rule 3 (Ongoing Membership Requirements) of the MBSD Rules, Rule 3A (Cash Settlement Bank Members) of the MBSD Rules and Section 8 of Rule 1 (Requirements Applicable to EPN Users) of Article III of the EPN Rules to require each Member to complete and deliver a Cybersecurity Confirmation at least every two years, on a date that is set by FICC and following notice that is provided no later than 180 calendar days prior to such due date.

(iv) *Implementation Timeframe*

Subject to approval by the Securities and Exchange Commission ("Commission"), the proposed rule change would become effective immediately. The proposed requirement that applicants deliver a Cybersecurity Confirmation with their application materials would be implemented immediately and would apply to applications that have been submitted at that time but have not yet been approved or rejected. Following the effective date of the proposed rule change, FICC would provide Members with notice of the due date of their Cybersecurity Confirmations, no later than 180 days prior to such due date, and would provide such notice at least every two years going forward.

(b) Statutory Basis

FICC believes the proposed rule changes are consistent with the requirements of the Act and the rules and regulations thereunder applicable to a registered clearing agency. In particular, FICC believes that the proposed rule changes are consistent with Section 17A(b)(3)(F) of the

Act,[9] and Rules 17Ad-22(e)(17)(i) and (e)(17)(ii), each promulgated under the Act,[10] for the reasons described below.

Section 17A(b)(3)(F) of the Act requires that the rules of FICC be designed to, among other things, promote the prompt and accurate clearance and settlement of securities transactions and assure the safeguarding of securities and funds which are in the custody or control of the clearing agency or for which it is responsible.[11]

As described above, the proposed requirement that Members and applicants provide a Cybersecurity Confirmation regarding their cybersecurity program that includes the representations described above would provide FICC with evidence of each Member's or applicant's management of endpoint security with respect to the SMART network or other connectivity and would enhance the protection of FICC against cyberattacks. The proposed Cybersecurity Confirmation would provide FICC with information that it could use to make decisions about risks or threats, perform additional monitoring, target potential vulnerabilities, and protect the FICC network. The proposed Cybersecurity Confirmation would give FICC the ability to further identify its exposure and enable it to take steps to mitigate risks. These requirements would help reduce risk to FICC's network with respect to its communications with Members and their submission of instructions and transactions to FICC by requiring all Members connecting to FICC to have appropriate cybersecurity programs in place.

Risks, threats and potential vulnerabilities could impact FICC's ability to clear and settle securities transactions, or to safeguard the securities and funds which are in its custody or control, or for which it is responsible. Therefore, by implementing a tool that would help to mitigate these risks, FICC believes the proposal would promote the prompt and accurate clearance and settlement of securities transactions and assure the safeguarding of securities and funds which are in the custody or control of the clearing agency or for which it is responsible, consistent with the requirements of Section 17A(b)(3)(F) of the Act.[12]

Rule 17Ad-22(e)(17)(i) under the Act requires that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to manage the covered clearing agency's operational risks by identifying the plausible sources of operational risk, both internal and external, and mitigating their impact through the use of appropriate systems, policies, procedures, and controls.[13] The proposed Cybersecurity Confirmation would reduce cybersecurity risks to FICC by requiring all Members and applicants to confirm they have defined and maintain cybersecurity programs that meet standard industry

---

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

10 17 CFR 240.17Ad-22(e)(17)(i) and (e)(17)(ii).

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

12 Id.

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

best practices and guidelines. The proposed representations in the Cybersecurity Confirmations would help FICC to mitigate its exposure to cybersecurity risk and, thereby, decrease the operational risks to FICC that are presented by connections to FICC through the SMART network or otherwise. The proposed Cybersecurity Confirmations would identify to FICC potential sources of external operational risks and enable it to mitigate these risks and their possible impacts to FICC's operations. As a result, FICC believes the proposal is consistent with the requirements of Rule 17Ad-22(e)(17)(i) under the Act.[14]

Rule 17Ad-22(e)(17)(ii) under the Act requires that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to manage the covered clearing agency's operational risks by ensuring, in part, that systems have a high degree of security, resiliency, and operational reliability.[15] The proposed Cybersecurity Confirmation would enhance the security, resiliency, and operational reliability of the endpoint security with respect to the SMART network or other connectivity because, as noted above, by making the Cybersecurity Confirmation an application requirement and an ongoing membership requirement, FICC would be able to prevent the connection by any applicant, and take action against any Member, that may pose an increased cyber risk to FICC by not having a defined and ongoing cybersecurity program that meets appropriate standards. Members or applicants that are not in alignment with a recognized framework, guideline, or standard that FICC believes is adequate to guide and assess such organization's cybersecurity program may present increased risk to FICC. By enabling FICC to identify these risks, the proposed changes would allow FICC to more effectively secure its environment against potential vulnerabilities. FICC's controls are strengthened when FICC's Members have similar technology risk management controls and programs within their computing environment. Control weaknesses within a Member's environment could allow for malicious or unauthorized usage of the link between FICC and the Member. As a result, FICC believes the proposal would improve FICC's ability to ensure that its systems have a high degree of security, resiliency, and operational reliability, and, as such, is consistent with the requirements of Rule 17Ad-22(e)(17)(ii) under the Act.[16]

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

FICC believes the proposed rule change could have an impact on competition. Specifically, FICC believes that the proposed rule change could burden competition because it would require Members and applicants that do not already have cybersecurity programs that meet the standards set out in the Cybersecurity Confirmation to incur additional costs including, but not limited to, establishing a cybersecurity program and framework, engaging an internal audit function or appropriate third party to review that program and framework, and remediating any findings from such review. In addition, those Members and applicants that do not connect directly to the SMART network, but connect through a third party service provider or service

---

14 Id.

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

16 Id.

bureau would have the additional burden of evaluating the cyber risks and impact of these third parties and reviewing the third party's assurance reports.

FICC believes the above described burden on competition that could be created by the proposed changes would be both necessary and appropriate in furtherance of the purposes of the Act, as permitted by Section 17A(b)(3)(I) of the Act, for the reasons described below.[17]

First, FICC believes the proposed rule change would be necessary in furtherance of the Act, specifically Section 17A(b)(3)(F) of the Act, because the Rules must be designed to promote the prompt and accurate clearance and settlement of securities transactions and assure the safeguarding of securities and funds which are in the custody or control of the clearing agency or for which it is responsible.[18] By requiring that Members and applicants provide a Cybersecurity Confirmation, the proposed rule change would allow FICC to better understand, assess, and, therefore, mitigate the cyber risks that FICC could face through its connections to its Members. As described above, these risks could impact FICC's ability to clear and settle securities transactions, or to safeguard the securities and funds which are in FICC's custody or control, or for which it is responsible. Implementing a tool as described above would help to mitigate these risks, and therefore FICC believes the proposal is necessary in furtherance of the requirements of Section 17A(b)(3)(F) of the Act.[19]

The proposed changes are also necessary in furtherance of the purposes of Rules 17Ad-22(e)(17)(i) and (e)(17)(ii) under the Act.[20] The proposed Cybersecurity Confirmations would identify to FICC potential sources of external operational risks and allow it to establish appropriate controls that would mitigate these risks and their possible impacts to FICC's operations. The proposed changes would also improve FICC's ability to ensure that its systems have a high degree of security, by enabling FICC to identify the cybersecurity risks that may be presented to it by Members that connect to FICC.

Second, FICC believes that the proposed rule change would be appropriate in furtherance of the purposes of the Act. The proposed rule change would apply equally to all Members and applicants. As described above, FICC believes Members may already be subject to one or more regulatory requirements that include the implementation of a cybersecurity program, and these firms would already follow a widely recognized framework, guideline, or standard, to guide and assess their organization's cybersecurity program to comply with these regulations. Therefore, FICC believes any burden that may be imposed by the proposed rule change would be appropriate.

Further, while the proposed Cybersecurity Confirmation would identify certain standards and guidelines that would be appropriate, FICC would consider requests by applicants and

---

17 15 U.S.C. 78q-1(b)(3)(I).

18 15 U.S.C. 78q-1(b)(3)(F).

19 Id.

20 17 CFR 240.17Ad-22(e)(17)(i) and (e)(17)(ii).

Members to allow other standards in accepting a Cybersecurity Confirmation. Additionally, the proposed Cybersecurity Confirmation would provide differing options to conduct the review of the applicant's or Member's cybersecurity program. As such, FICC has endeavored to design the Cybersecurity Confirmation in a way that is reasonable and does not require one approach for meeting its requirements.

Finally, FICC is proposing to provide Members with a minimum of 180 calendar days' notice before the deadline for providing a Cybersecurity Confirmation. This notice would allow Members to address any impact this change may have on their business. Applicants would be required to provide the Cybersecurity Confirmation as part of their application materials upon the effective date of this proposed rule change. This implementation schedule is designed to be fair and not disproportionately impact any Members more than others. The proposal is designed to provide all impacted Members with time to review their cybersecurity programs with respect to the required representations, and identify, if necessary, internal or third party cybersecurity reviewers.

For the reasons described above, FICC believes any burden on competition that may result from the proposed rule change would be both necessary and appropriate in furtherance of the purposes of the Act, as permitted by Section 17A(b)(3)(I) of the Act.[21]

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

FICC has not solicited or received any written comments relating to this proposal. FICC will notify the Commission of any written 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[22] for Commission action.

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

(a) Not applicable.

(b) Not applicable.

(c) Not applicable.

(d) Not applicable.

---

21 15 U.S.C. 78q-1(b)(3)(I).

22 15 U.S.C. 78s(b)(2).

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

Not applicable.

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

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 – FICC Cybersecurity Confirmation form.

Exhibit 4 – Not applicable.

Exhibit 5 – Proposed changes to the Rules.

EXHIBIT 1A

SECURITIES AND EXCHANGE COMMISSION
(Release No. 34-[_____]; File No. SR-FICC-2019-005)

[DATE]

Self-Regulatory Organizations; Fixed Income Clearing Corporation; Notice of Filing of Proposed Rule Change to Require Confirmation of Cybersecurity Program

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 October __, 2019, 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 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] in order to (1) define "Cybersecurity Confirmation"

---

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

as a signed, written representation that addresses the submitting firm's cybersecurity program; and (2) enhance the GSD and MBSD application requirements and ongoing requirements for Members to (a) require that a Cybersecurity Confirmation be provided as part of the application materials for all Members, and (b) require that all Members deliver to FICC a complete, updated Cybersecurity Confirmation at least every two years, 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

(i) *Overview*

FICC is proposing to modify the Rules in order to (1) define "Cybersecurity Confirmation" as a signed, written representation that addresses the submitting firm's cybersecurity program; and (2) enhance the GSD and MBSD application requirements and ongoing requirements for Members to (a) require that a Cybersecurity Confirmation be provided as part of the application materials for all Members, and (b) require that all Members deliver to FICC a complete, updated Cybersecurity Confirmation at least every two years.

The proposed change would require all Members and applicants to deliver to FICC a signed, written Cybersecurity Confirmation, which includes representations regarding the submitting firm's cybersecurity program and framework. The Cybersecurity Confirmation would be required to be (1) delivered with the application materials for every applicant, and (2) updated and re-delivered at least every two years by all Members.

As described in more detail below, the Cybersecurity Confirmation would help FICC to assess the cybersecurity risks that may be introduced to it by Members that connect to FICC either through the Securely Managed and Reliable Technology ("SMART") network[4] or through other connections. The proposed Cybersecurity Confirmation would allow FICC to better understand its Members' cybersecurity programs and frameworks and identify possible cybersecurity risk exposures. Based on this information, FICC would be able to establish appropriate controls to mitigate these risks and their possible impacts to FICC's operations.

(ii) *Background of Proposal*

FICC believes it is prudent to better understand the cybersecurity risks that it may face through its interconnections to Members. As a designated systemically important financial market utility, or "SIFMU," FICC occupies a unique position in the marketplace such that a failure or a disruption to FICC could increase the risk of significant liquidity

---

[4] The SMART network is a technology managed by FICC's parent company, The Depository Trust & Clearing Corporation ("DTCC"), that connects a nationwide complex of networks, processing centers and control facilities. This network extends between FICC's and its Members' operating premises. DTCC operates on a shared services model with respect to FICC and DTCC's other subsidiaries pursuant to intercompany agreements under which it is generally DTCC that provides a relevant service to its subsidiaries, including FICC.

problems spreading among financial institutions or markets and thereby threaten the stability of the financial system in the United States.[5] Given its designation as a SIFMU, FICC believes it is prudent to develop an enhanced endpoint security framework designed so that its SMART network or other connectivity is adequately protected against cyberattacks.

Currently, FICC does not obtain any information regarding the security of a firm's systems or cybersecurity program prior to permitting that firm to connect either directly to the SMART network or to FICC through another means, such as through a third party service provider, service bureau, network, or the Internet. Given FICC's critical role in the marketplace, FICC is proposing to address the risks that could be posed by these connections.

Members may currently be subject to regulations that are designed, in part, to enhance the safeguards used by these entities to protect themselves against cyberattacks.[6] In order to comply with such regulations, Members and applicants would be required to

---

5 FICC and its affiliates, The Depository Trust Company and National Securities Clearing Corporation, were designated SIFMUs under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010. 12 U.S.C. 5465(e)(1).

6 For example, depending on the type of entity, Members may be subject to one or more of the following regulations: (1) Regulation S-ID, which requires "financial institutions" or "creditors" under the rule to adopt programs to identify and address the risk of identity theft of individuals (17 CFR 248.201 - 202); (2) Regulation S-P, which requires broker-dealers, investment companies, and investment advisers to adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information (17 CFR 248.1 - 30); and (3) Rule 15c3-5 under the Act, known as the "Market Access Rule," which requires broker-dealers to establish, document, and maintain a system for regularly reviewing the effectiveness of its management controls and supervisory procedures (17 CFR 240.15c3-5).

follow standards established by national or international organizations focused on information security management, and would have already established protocols to allow their senior management to verify that they have sufficient cybersecurity programs in place to fulfill existing regulatory obligations. Other Members have established and follow substantially similar protocols because of evolving expectations by regulators or by institutional customers as to the sufficiency of their cyber safeguards. FICC believes that it should require confirmation of the cybersecurity standards utilized by its Members and applicants that connect to its network.

The proposed Cybersecurity Confirmation would require Members and applicants to represent that they have established adequate controls and security to help limit (1) cybersecurity risks to FICC and to the other Members' networks and (2) access by unauthorized third parties while the firm is connected to FICC either directly through the SMART network or through other connectivity such as a service provider, service bureau, network, or the Internet.

(iii) *Proposed Rule Changes*

FICC is proposing to modify its Rules to (1) define "Cybersecurity Confirmation;" and (2) require that firms deliver a completed Cybersecurity Confirmation (a) as part of their initial application with FICC, and (b) on an ongoing basis, at least every two years. Each of these proposed rule changes is described in greater detail below.

(1) *Proposed Cybersecurity Confirmation*

FICC is proposing to adopt a definition of "Cybersecurity Confirmation." Each Cybersecurity Confirmation would be required to be in writing on a form provided by

FICC and signed by a designated senior executive of the submitting firm who is authorized to attest to these matters. Based on the form provided by FICC, each Cybersecurity Confirmation would contain representations regarding the submitting firm's cybersecurity program and framework. Such representations by the submitting firm would cover the two years prior to the date of the most recently provided Cybersecurity Confirmation.

FICC is proposing to require that the following representations be included in the form of Cybersecurity Confirmation:

First, the Cybersecurity Confirmation would include a representation that the submitting firm has defined and maintains a comprehensive cybersecurity program and framework that considers potential cyber threats that impact the organization and protects the confidentiality, integrity and availability requirements of its systems and information.

Second, the Cybersecurity Confirmation would include a representation that the submitting firm has implemented and maintains a written enterprise cybersecurity policy or policies approved by the submitting firm's senior management or board of directors, and the organization's cybersecurity framework is in alignment with standard industry best practices and guidelines.[7]

---

[7] Examples of recognized frameworks, guidelines and standards that FICC believes are adequate include the Financial Services Sector Coordinating Council Cybersecurity Profile, the National Institute of Standards and Technology Cybersecurity Framework ("NIST CSF"), International Organization for Standardization ("ISO") standard 27001/27002 ("ISO 27001"), Federal Financial Institutions Examination Council ("FFIEC") Cybersecurity Assessment Tool, Critical Security Controls Top 20, and Control Objectives for Information and Related Technologies. FICC would identify recognized frameworks, guidelines and standards in the form of Cybersecurity Confirmation and in an Important Notice that FICC would issue from time to time. FICC would also consider accepting other standards upon request by a Member or applicant.

Third, the Cybersecurity Confirmation would include a representation that, if the submitting firm is using a third party service provider or service bureau(s) to connect or transact business or to manage the connection with FICC, the submitting firm has an appropriate program to (a) evaluate the cyber risks and impact of these third parties, and (b) review the third party assurance reports.

Fourth, the Cybersecurity Confirmation would include a representation that the submitting firm's cybersecurity program and framework protect the segment of their system that connects to and/or interacts with FICC.

Fifth, the Cybersecurity Confirmation would include a representation that the submitting firm has in place an established process to remediate cyber issues identified to fulfill the submitting firm's regulatory and/or statutory requirements.

Sixth, the Cybersecurity Confirmation would include a representation that the submitting firm's cybersecurity program's and framework's risk processes are updated periodically based on a risk assessment or changes to technology, business, threat ecosystem, and/or regulatory environment.

And, finally, the Cybersecurity Confirmation would include a representation that the review of the submitting firm's cybersecurity program and framework has been conducted by one of the following: (1) the submitting firm, if it has filed and maintains a current Certification of Compliance with the Superintendent of the New York State Department of Financial Services confirming compliance with its Cybersecurity Requirements for Financial Services Companies;[8] (2) a regulator who assesses the

---

[8] 23 N.Y. Comp. Codes R. & Regs. tit. 23, § 500 (2017). This regulation requires firms to confirm that they have a comprehensive cybersecurity program, as

program against an industry cybersecurity framework or industry standard, including those that are listed on the form of Cybersecurity Confirmation and in an Important Notice that is issued by FICC from time to time;[9] (3) an independent external entity with cybersecurity domain expertise in relevant industry standards and practices, including those that are listed on the form of Cybersecurity Confirmation and in an Important Notice that is issued by FICC from time to time;[10] or (4) an independent internal audit function reporting directly to the submitting firm's board of directors or designated board of directors committee, such that the findings of that review are shared with these governance bodies.

Together, the required representations are designed to provide FICC with evidence of each Member's or applicant's management of cybersecurity with respect to their connectivity to FICC. By requiring these representations from Members and applicants, the proposed Cybersecurity Confirmation would provide FICC with

---

described in the regulation, which FICC believes is sufficient to meet the objectives of the proposed Cybersecurity Confirmation.

9 Industry cybersecurity frameworks and industry standards could include, for example, the Office of the Comptroller of the Currency or the FFIEC Cybersecurity Assessment Tool. FICC would identify acceptable industry cybersecurity frameworks and standards in the form of Cybersecurity Confirmation and in an Important Notice that FICC would issue from time to time. FICC would also consider accepting other industry cybersecurity frameworks and standards upon request by a Member or applicant.

10 A third party with cybersecurity domain expertise is one that follows and understands industry standards, practices and regulations that are relevant to the financial sector. Examples of such standards and practices include ISO 27001 certification or NIST CSF assessment. FICC would identify acceptable industry standards and practices in the form of Cybersecurity Confirmation and in an Important Notice that FICC would issue from time to time. FICC would also consider accepting other industry standards and practices upon request by a Member or applicant.

information that it could use to make decisions about risks or threats, perform additional monitoring, target potential vulnerabilities, and protect the FICC network.

FICC is proposing to amend Rule 1 (Definitions) of the GSD Rules, Rule 1 (Definitions) of the MBSD Rules, and Rule 1 (Definitions) of Article I (Definitions and General Provisions) of the EPN Rules, to include a definition of "Cybersecurity Confirmation" as described above.

(2) *Initial and Ongoing Membership Requirement*

FICC is proposing to require that a Cybersecurity Confirmation be submitted to FICC by any applicant, as part of their application materials, and at least every two years by all Members. With respect to the requirement to deliver a Cybersecurity Confirmation at least every two years, FICC would provide all Members with notice of the date on which such Cybersecurity Confirmations would be due no later than 180 calendar days prior to such due date.

In order to implement these proposed changes, FICC would amend Section 5 of Rule 2A (Initial Membership Requirements) of the GSD Rules, Section 3 of Rule 3B (Centrally Cleared Institutional Triparty Service) of the GSD Rules, Section 4 of Rule 13 (Funds-Only Settlement) of the GSD Rules, Section 3 of Rule 2A (Initial Membership Requirements) of the MBSD Rules, Rule 3A (Cash Settlement Bank Members) of the MBSD Rules, and Section 2 of Rule 1 (Requirements Applicable to EPN Users) of Article III of the EPN Rules to require that applicants complete and deliver a Cybersecurity Confirmation as part of their application materials.

Further, FICC would amend Section 2 of Rule 3 (Ongoing Membership Requirements) of the GSD Rules, Section 5 of Rule 3B (Centrally Cleared Institutional

Triparty Service) of the GSD Rules, Section 4 of Rule 13 (Funds-Only Settlement) of the GSD Rules, Section 2 of Rule 3 (Ongoing Membership Requirements) of the MBSD Rules, Rule 3A (Cash Settlement Bank Members) of the MBSD Rules and Section 8 of Rule 1 (Requirements Applicable to EPN Users) of Article III of the EPN Rules to require each Member to complete and deliver a Cybersecurity Confirmation at least every two years, on a date that is set by FICC and following notice that is provided no later than 180 calendar days prior to such due date.

(iv) *Implementation Timeframe*

Subject to approval by the Commission, the proposed rule change would become effective immediately. The proposed requirement that applicants deliver a Cybersecurity Confirmation with their application materials would be implemented immediately and would apply to applications that have been submitted at that time but have not yet been approved or rejected. Following the effective date of the proposed rule change, FICC would provide Members with notice of the due date of their Cybersecurity Confirmations, no later than 180 days prior to such due date, and would provide such notice at least every two years going forward.

2. Statutory Basis

FICC believes the proposed rule changes are consistent with the requirements of the Act and the rules and regulations thereunder applicable to a registered clearing agency. In particular, FICC believes that the proposed rule changes are consistent with

Section 17A(b)(3)(F) of the Act,[11] and Rules 17Ad-22(e)(17)(i) and (e)(17)(ii), each promulgated under the Act,[12] for the reasons described below.

Section 17A(b)(3)(F) of the Act requires that the rules of FICC be designed to, among other things, promote the prompt and accurate clearance and settlement of securities transactions and assure the safeguarding of securities and funds which are in the custody or control of the clearing agency or for which it is responsible.[13]

As described above, the proposed requirement that Members and applicants provide a Cybersecurity Confirmation regarding their cybersecurity program that includes the representations described above would provide FICC with evidence of each Member's or applicant's management of endpoint security with respect to the SMART network or other connectivity and would enhance the protection of FICC against cyberattacks. The proposed Cybersecurity Confirmation would provide FICC with information that it could use to make decisions about risks or threats, perform additional monitoring, target potential vulnerabilities, and protect the FICC network. The proposed Cybersecurity Confirmation would give FICC the ability to further identify its exposure and enable it to take steps to mitigate risks. These requirements would help reduce risk to FICC's network with respect to its communications with Members and their submission of instructions and transactions to FICC by requiring all Members connecting to FICC to have appropriate cybersecurity programs in place.

---

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

12 17 CFR 240.17Ad-22(e)(17)(i) and (e)(17)(ii).

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

Risks, threats and potential vulnerabilities could impact FICC's ability to clear and settle securities transactions, or to safeguard the securities and funds which are in its custody or control, or for which it is responsible. Therefore, by implementing a tool that would help to mitigate these risks, FICC believes the proposal would promote the prompt and accurate clearance and settlement of securities transactions and assure the safeguarding of securities and funds which are in the custody or control of the clearing agency or for which it is responsible, consistent with the requirements of Section 17A(b)(3)(F) of the Act.[14]

Rule 17Ad-22(e)(17)(i) under the Act requires that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to manage the covered clearing agency's operational risks by identifying the plausible sources of operational risk, both internal and external, and mitigating their impact through the use of appropriate systems, policies, procedures, and controls.[15] The proposed Cybersecurity Confirmation would reduce cybersecurity risks to FICC by requiring all Members and applicants to confirm they have defined and maintain cybersecurity programs that meet standard industry best practices and guidelines. The proposed representations in the Cybersecurity Confirmations would help FICC to mitigate its exposure to cybersecurity risk and, thereby, decrease the operational risks to FICC that are presented by connections to FICC through the SMART network or otherwise. The proposed Cybersecurity Confirmations would identify to FICC potential sources of external operational risks and enable it to mitigate these risks and their

---

14 Id.

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

possible impacts to FICC's operations. As a result, FICC believes the proposal is consistent with the requirements of Rule 17Ad-22(e)(17)(i) under the Act.[16]

Rule 17Ad-22(e)(17)(ii) under the Act requires that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to manage the covered clearing agency's operational risks by ensuring, in part, that systems have a high degree of security, resiliency, and operational reliability.[17] The proposed Cybersecurity Confirmation would enhance the security, resiliency, and operational reliability of the endpoint security with respect to the SMART network or other connectivity because, as noted above, by making the Cybersecurity Confirmation an application requirement and an ongoing membership requirement, FICC would be able to prevent the connection by any applicant, and take action against any Member, that may pose an increased cyber risk to FICC by not having a defined and ongoing cybersecurity program that meets appropriate standards. Members or applicants that are not in alignment with a recognized framework, guideline, or standard that FICC believes is adequate to guide and assess such organization's cybersecurity program may present increased risk to FICC. By enabling FICC to identify these risks, the proposed changes would allow FICC to more effectively secure its environment against potential vulnerabilities. FICC's controls are strengthened when FICC's Members have similar technology risk management controls and programs within their computing environment. Control weaknesses within a Member's environment could allow for malicious or unauthorized usage of the link between FICC and the Member. As a result, FICC

---

16 Id.

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

believes the proposal would improve FICC's ability to ensure that its systems have a high degree of security, resiliency, and operational reliability, and, as such, is consistent with the requirements of Rule 17Ad-22(e)(17)(ii) under the Act.[18]

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

FICC believes the proposed rule change could have an impact on competition. Specifically, FICC believes that the proposed rule change could burden competition because it would require Members and applicants that do not already have cybersecurity programs that meet the standards set out in the Cybersecurity Confirmation to incur additional costs including, but not limited to, establishing a cybersecurity program and framework, engaging an internal audit function or appropriate third party to review that program and framework, and remediating any findings from such review. In addition, those Members and applicants that do not connect directly to the SMART network, but connect through a third party service provider or service bureau would have the additional burden of evaluating the cyber risks and impact of these third parties and reviewing the third party's assurance reports.

FICC believes the above described burden on competition that could be created by the proposed changes would be both necessary and appropriate in furtherance of the purposes of the Act, as permitted by Section 17A(b)(3)(I) of the Act, for the reasons described below.[19]

First, FICC believes the proposed rule change would be necessary in furtherance of the Act, specifically Section 17A(b)(3)(F) of the Act, because the Rules must be

---

18 Id.

19 15 U.S.C. 78q-1(b)(3)(I).

designed to promote the prompt and accurate clearance and settlement of securities transactions and assure the safeguarding of securities and funds which are in the custody or control of the clearing agency or for which it is responsible.[20] By requiring that Members and applicants provide a Cybersecurity Confirmation, the proposed rule change would allow FICC to better understand, assess, and, therefore, mitigate the cyber risks that FICC could face through its connections to its Members. As described above, these risks could impact FICC's ability to clear and settle securities transactions, or to safeguard the securities and funds which are in FICC's custody or control, or for which it is responsible. Implementing a tool as described above would help to mitigate these risks, and therefore FICC believes the proposal is necessary in furtherance of the requirements of Section 17A(b)(3)(F) of the Act.[21]

The proposed changes are also necessary in furtherance of the purposes of Rules 17Ad-22(e)(17)(i) and (e)(17)(ii) under the Act.[22] The proposed Cybersecurity Confirmations would identify to FICC potential sources of external operational risks and allow it to establish appropriate controls that would mitigate these risks and their possible impacts to FICC's operations. The proposed changes would also improve FICC's ability to ensure that its systems have a high degree of security, by enabling FICC to identify the cybersecurity risks that may be presented to it by Members that connect to FICC.

Second, FICC believes that the proposed rule change would be appropriate in furtherance of the purposes of the Act. The proposed rule change would apply equally to

---

20 15 U.S.C. 78q-1(b)(3)(F).

21 Id.

22 17 CFR 240.17Ad-22(e)(17)(i) and (e)(17)(ii).

all Members and applicants. As described above, FICC believes Members may already be subject to one or more regulatory requirements that include the implementation of a cybersecurity program, and these firms would already follow a widely recognized framework, guideline, or standard, to guide and assess their organization's cybersecurity program to comply with these regulations. Therefore, FICC believes any burden that may be imposed by the proposed rule change would be appropriate.

Further, while the proposed Cybersecurity Confirmation would identify certain standards and guidelines that would be appropriate, FICC would consider requests by applicants and Members to allow other standards in accepting a Cybersecurity Confirmation. Additionally, the proposed Cybersecurity Confirmation would provide differing options to conduct the review of the applicant's or Member's cybersecurity program. As such, FICC has endeavored to design the Cybersecurity Confirmation in a way that is reasonable and does not require one approach for meeting its requirements.

Finally, FICC is proposing to provide Members with a minimum of 180 calendar days' notice before the deadline for providing a Cybersecurity Confirmation. This notice would allow Members to address any impact this change may have on their business. Applicants would be required to provide the Cybersecurity Confirmation as part of their application materials upon the effective date of this proposed rule change. This implementation schedule is designed to be fair and not disproportionately impact any Members more than others. The proposal is designed to provide all impacted Members with time to review their cybersecurity programs with respect to the required representations, and identify, if necessary, internal or third party cybersecurity reviewers.

For the reasons described above, FICC believes any burden on competition that may result from the proposed rule change would be both necessary and appropriate in furtherance of the purposes of the Act, as permitted by Section 17A(b)(3)(I) of the Act.[23]

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

FICC has not solicited or received any written comments relating to this proposal. FICC will notify the Commission of any written 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 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

---

[23] 15 U.S.C. 78q-1(b)(3)(I).

- Send an e-mail to rule-comments@sec.gov. Please include File Number SR-FICC-2019-005 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-2019-005. 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-2019-005 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.[24]

Secretary

[24] 17 CFR 200.30-3(a)(12).

EXHIBIT 3

CONFIRMATION OF A CLIENT CYBERSECURITY PROGRAM
FICC

Fixed Income Clearing Corporation
The Depository Trust & Clearing Corporation
55 Water Street
New York, NY 10041

Client Legal Entity Name: _____ ("The Company")

Attention: Control Officer Name: _____

Which standards and/or frameworks are you using to guide and assess your institution's cybersecurity program? Please select all that apply.

☐	**FSSCC Profile**	Financial Services Sector Coordinating Council Cybersecurity Profile
☐	**NIST CSF**	The National Institute of Standards and Technology Cybersecurity Framework
☐	**ISO 27001/27002**	International Organization for Standardization Standard 27001/27002
☐	**FFIEC CAT**	Federal Financial Institutions Examination Council Cybersecurity Assessment Tool
☐	**CSC 20**	Critical Security Controls Top 20
☐	**COBIT**	Control Objectives for Information and Related Technologies
☐	**Other**	

Are you using a third party service provider or service bureau to access Fixed Income Clearing Corporation ("FICC")?

CONFIRMATION

The Company has designated the senior executive indicated below with sufficient authority to be responsible and accountable for overseeing and executing the cybersecurity program within the organization.

- The Company has defined and maintains a comprehensive cybersecurity program and framework that considers potential cyber threats that impact the organization and protects the confidentiality, integrity and availability requirements of The Company's systems and information.

- The Company has implemented and maintains a written enterprise cybersecurity policy or policies approved by senior management or The Company's board of directors, and The Company's cybersecurity framework is in alignment with standard industry best practices and guidelines as indicated: (FSSCC Profile, NIST CSF, ISO 27001/27002, FFIEC CAT, CSC 20, COBIT).

- If using a third party service provider or service bureau(s) to connect or transact business or to manage the connection with FICC, The Company has an appropriate program to evaluate the cyber risks and impact of these third parties, and to review the third party assurance reports.

- The Company's cybersecurity program and framework protect the segment of The Company's system that connects to and/or interacts with FICC.
- There is an established process to remediate cyber issues identified to fulfill regulatory and/or statutory requirements.
- The Company's cybersecurity program's and framework's risk processes are updated periodically based on a risk assessment or changes to technology, business, threat ecosystem, and regulatory environment.
- A comprehensive review of the cybersecurity program and framework has been conducted by one of the following:
    - ☐ The Company, which has filed and maintains a current Certification of Compliance with the Superintendent of the New York State Department of Financial Services (NYSDFS) pursuant to 23 NYCRR 500
    - ☐ A regulator who assesses the program against a designated cybersecurity framework or industry standard (OCC: Office of the Comptroller and the FFIEC CAT)
    - ☐ An independent external entity with cybersecurity domain expertise (SOC2 Certification, ISO 27001 Certification, NIST CSF assessment)
    - ☐ An independent internal audit function reporting directly to the board of directors or designated board of directors committee of The Company, such that the findings of that review are shared with these governance bodies

I am the designated senior executive authorized to attest to the above on behalf of The Company.

CONTROL OFFICER:

First Name: _____ **Last Name:** _____

Phone: _____ **Email:** _____

Title _____ **Date** _____

Signature: _____

EXHIBIT 5

FIXED INCOME CLEARING CORPORATION

GOVERNMENT SECURITIES DIVISION RULEBOOK

TEXT OF PROPOSED RULE CHANGE

Bold and underlined text indicates proposed added language.

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

RULE 1 – DEFINITIONS

* * *

Cybersecurity Confirmation

The term "Cybersecurity Confirmation" means a written document provided to the Corporation by all Members, Sponsoring Members and CCIT Members (for purposes of this definition, collectively referred to as "Members") and applicants for such membership that confirms the existence of an information system cybersecurity program and includes the representations listed below.

Each Cybersecurity Confirmation shall (1) be on a form provided by the Corporation; (2) be signed by a designated senior executive of the Member or applicant who is authorized to attest to these matters; and (3) include the following representations, made with respect to the two years prior to the date of the Cybersecurity Confirmation:

1. **The Member or applicant has defined and maintains a comprehensive cybersecurity program and framework that considers potential cyber threats that impact their organization and protects the confidentiality, integrity and availability requirements of their systems and information.**

2. **The Member or applicant has implemented and maintains a written enterprise cybersecurity policy or policies approved by senior management or the organization's board of directors, and the organization's cybersecurity framework is in alignment with standard industry best practices and guidelines, as indicated on the form of Cybersecurity Confirmation.**

3. **If using a third party service provider or service bureau(s) to connect or transact business or to manage the connection with the Corporation, the Member or applicant has an appropriate program to (a) evaluate the cyber risks and impact of these third-parties, and (b) review the third-party assurance reports.**

4. **The cybersecurity program and framework protect the segment of the Member's or applicant's system that connects to and/or interacts with the Corporation.**

5. **The Member or applicant has in place an established process to remediate cyber issues identified to fulfill the Member's or applicant's regulatory and/or statutory requirements.**

6. **The cybersecurity program's and framework's risk processes are updated periodically based on a risk assessment or changes to technology, business, threat ecosystem, and/or regulatory environment.**

7. A comprehensive review of the Member's or applicant's cybersecurity program and framework has been conducted by one of the following:

- **The Member or applicant, if that organization has filed and maintains a current Certification of Compliance with the Superintendent of the New York State Department of Financial Services pursuant to 23 NYCRR 500;**

- **A regulator who assesses the program against a designated cybersecurity framework or industry standard, including those that are listed on the form of the Cybersecurity Confirmation and in an Important Notice issued by the Corporation from time to time;**

- **An independent external entity with cybersecurity domain expertise, including those that are listed on the form of the Cybersecurity Confirmation and in an Important Notice issued by the Corporation from time to time; and**

- **An independent internal audit function reporting directly to the board of directors or designated board of directors committee of the Member or applicant, such that the findings of that review are shared with these governance bodies.**

* * *

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.

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

Each applicant to become a Member must also fulfill, within the time frames 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.

If the Corporation determines that a legal opinion, or update thereto, submitted by an applicant, indicates that the Corporation could be subject to Legal Risk (as defined in Section 2 of Rule 4) with respect to such applicant, the Corporation shall have the right to take, and/or require the applicant to take, appropriate action(s) to mitigate such Legal Risk, including, but not limited to, requiring the applicant to post additional Clearing Fund as set forth in Section 2 of Rule 4.

Except as otherwise provided in Rule 29, any information furnished to the Corporation pursuant to this Rule shall be held in at least the same degree of confidence as may be required by law or the rules and regulations of the appropriate regulatory body having jurisdiction over the applicant or Member.

* * *

RULE 3 – ONGOING MEMBERSHIP REQUIREMENTS

* * *

Section 2 – Reports by Netting Members

Each Netting Member shall submit to the Corporation the reports, financial or other information set forth below and such other reports, financial and other 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, on a periodic basis, GCF Counterparties must submit information related to the composition of their NFE-Related Accounts. This information shall be submitted to the Corporation containing the information, in the format and within the timeframes specified by guidelines issued by the Corporation from time to time.

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.

Notwithstanding anything to the contrary in this Rule, if a Member qualifies for more than one category of Netting 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.

* * *

RULE 3B – CENTRALLY CLEARED INSTITUTIONAL TRIPARTY SERVICE

* * *

Section 3 – Membership Application Process to Become a CCIT Member

* * *

(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) a Cybersecurity Confirmation.

* * *

Section 5 – On-going Membership Requirements

(a) The eligibility qualifications and standards set forth above in this Rule shall be continuing membership requirements. In addition, each CCIT Member shall comply with the ongoing requirements set forth below in this Section.

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

(i) 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) 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.

* * *

RULE 13 – FUNDS-ONLY SETTLEMENT

* * *

Section 4 – Funds-Only Settling Bank Members

* * *

(d) Each applicant in (b)(i), (b)(ii), (b)(iii) and (b)(iv) shall sign and deliver to the Corporation:

(i) a membership agreement whereby the bank or trust company shall agree to:

(1) abide by the Rules of the Corporation applicable to Funds-Only 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) be bound by any amendment to the Rules of the Corporation 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 the Rules of the Corporation.

(ii) the "Appointment of Funds-Only Settling Bank and Funds-Only Settling Bank Agreement"; ~~and~~

(iii) the agreement(s) authorizing the Corporation's Settlement Agent to utilize NSS for funds-only settlement as the relevant FRB may require**; and**

(iv) a Cybersecurity Confirmation.

* * *

(k) Each Funds-Only Settling Bank shall fulfill, within the timeframe 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 test results to the Corporation in a manner specified by the Corporation) that may be imposed by the Corporation from time to time to ensure the continuing operational capability of the Funds-Only Settling Bank.

(l) Each Funds-Only Settling Bank 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.

(~~l~~**m**) In addition to this Rule 13 and applicable provisions of Rule 1, the following Rules and any relevant schedules cited therein shall apply to Funds-Only Settling Bank Members in the same manner as they apply to Netting Members: Rule 22D (Wind-down of the Corporation), Rule

29 (Release of Clearing Data), Rule 32 (Signatures), Rule 33 (Procedures), Rule 36 (Rule Changes), Rule 37 (Hearing Procedures), Rule 38 (Governing Law and Captions), Rule 39 (Limitations of Liability), Rule 42 (Suspension of Rules), Rule 44 (Action by the Corporation), Rule 45 (Notices), Rule 46 (Interpretation of Terms), Rule 47 (Interpretation of Rules), Rule 48 (Disciplinary Proceedings), and Rule 50 (Market Disruption and Force Majeure).

* * *

FIXED INCOME CLEARING CORPORATION

MORTGAGE-BACKED SECURITIES DIVISION

CLEARING RULES

RULE 1 - DEFINITIONS

* * *

Cybersecurity Confirmation

The term "Cybersecurity Confirmation" means a written document provided to the Corporation by all Members and applicants for membership that confirms the existence of an information system cybersecurity program and includes the representations listed below.

Each Cybersecurity Confirmation shall (1) be on a form provided by the Corporation; (2) be signed by a designated senior executive of the Member or applicant who is authorized to attest to these matters; and (3) include the following representations, made with respect to the two years prior to the date of the Cybersecurity Confirmation:

1. **The Member or applicant has defined and maintains a comprehensive cybersecurity program and framework that considers potential cyber threats that impact their organization and protects the confidentiality, integrity and availability requirements of their systems and information.**

2. **The Member or applicant has implemented and maintains a written enterprise cybersecurity policy or policies approved by senior management or the organization's board of directors, and the organization's cybersecurity framework is in alignment with standard industry best practices and guidelines, as indicated on the form of Cybersecurity Confirmation.**

3. **If using a third party service provider or service bureau(s) to connect or transact business or to manage the connection with the Corporation, the Member or applicant has an appropriate program to (a) evaluate the cyber risks and impact of these third-parties, and (b) review the third-party assurance reports.**

4. **The cybersecurity program and framework protect the segment of the Member's or applicant's system that connects to and/or interacts with the Corporation.**

5. **The Member or applicant has in place an established process to remediate cyber issues identified to fulfill the Member's or applicant's regulatory and/or statutory requirements.**

6. **The cybersecurity program's and framework's risk processes are updated periodically based on a risk assessment or changes to technology, business, threat ecosystem, and/or regulatory environment.**

7. A comprehensive review of the Member's or applicant's cybersecurity program and framework has been conducted by one of the following:

- **The Member or applicant, if that organization has filed and maintains a current Certification of Compliance with the Superintendent of the New York State Department of Financial Services pursuant to 23 NYCRR 500;**

- **A regulator who assesses the program against a designated cybersecurity framework or industry standard, including those that are listed on the form of the Cybersecurity Confirmation and in an Important Notice issued by the Corporation from time to time;**

- **An independent external entity with cybersecurity domain expertise, including those that are listed on the form of the Cybersecurity Confirmation and in an Important Notice issued by the Corporation from time to time; and**

- **An independent internal audit function reporting directly to the board of directors or designated board of directors committee of the Member or applicant, such that the findings of that review are shared with these governance bodies.**

* * *

RULE 2A – INITIAL MEMBERSHIP REQUIREMENTS

* * *

Section 3 – Application Documents

Each applicant to become a Clearing 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 Clearing System shall also deliver to the Corporation the financial reports, other reports, opinions and other information as the Corporation requires.

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

If the Corporation determines that a legal opinion, or update thereto, submitted by an applicant indicates that the Corporation could be subject to Legal Risk as defined in Rule 4 with respect to such applicant, the Corporation shall have the right to take, and/or require the applicant to take, appropriate action(s) to mitigate such Legal Risk, including, but not limited to, requiring the applicant to post additional Clearing Fund as set forth in Rule 4.

* * *

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.

* * *

If the Corporation determines that a legal opinion, or update thereto, submitted by a Member, indicates that the Corporation could be subject to Legal Risk (as defined in Rule 4) with respect to such Member, the Corporation shall have the right to take, and/or require the Member to take, appropriate action(s) to mitigate such Legal Risk, including, but not limited to, requiring the Member to post additional Clearing Fund as set forth in Rule 4.

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.

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.

* * *

RULE 3A – CASH SETTLMENT BANK MEMBERS

* * *

(d) Each applicant in subsections (b)(i) through (b)(iv) shall sign and deliver to the Corporation:

(i) a membership agreement whereby the bank or trust company shall agree to:

(1) abide by the Rules of the Corporation 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) be bound by any amendment to the Rules of the Corporation 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 the Rules of the Corporation.

(ii) the "Appointment of Cash Settling Bank and Cash Settling Bank Agreement"; ~~and~~

(iii) the agreement(s) authorizing the Corporation's Settlement Agent to utilize NSS for cash settlement as the relevant FRB may require**; and**

(iv) a Cybersecurity Confirmation.

* * *

(k) Each Cash Settling Bank shall fulfill, within the timeframe 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 test results to the Corporation in a manner specified by the Corporation) that may be imposed by the Corporation from time to time to ensure the continuing operational capability of the Cash Settling Bank.

(l) Each Cash Settling Bank 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.

(~~l~~**m**) In addition to the applicable provisions of these Rules where Cash Settling Bank Members are mentioned, the following Rules and any relevant schedules cited therein shall apply to Cash Settling Bank Members in the same manner as they apply to Members: Rule 17B, "Winddown of the Corporation," Rule 22, "Release of Clearing Data," Rule 24, "Signatures," Rule 27, "Rule Changes," Rule 28, "Hearing Procedures," Rule 29, "Governing Law and Captions," Rule 30, "Limitations of Liability," Rule 33, "Suspension of Rules in Emergency Circumstances," Rule 34, "Action by the Corporation," Rule 35, "Notices," Rule 36, "Interpretation of Terms," Rule 37, "Interpretation of Rules," Rule 38 "Disciplinary Proceedings," and Rule 40 "Market Disruption and Force Majeure."

* * *

FIXED INCOME CLEARING CORPORATION

MORTGAGE-BACKED SECURITIES DIVISION

EPN RULES

ARTICLE I
DEFINITIONS AND GENERAL PROVISIONS

Rule 1. Definitions

* * *

Cybersecurity Confirmation

The term "Cybersecurity Confirmation" means a written document provided to the Corporation by all EPN Users and applicants that confirms the existence of an information system cybersecurity program and includes the representations listed below.

Each Cybersecurity Confirmation shall (1) be on a form provided by the Corporation; (2) be signed by a designated senior executive of the EPN User or applicant who is authorized to attest to these matters; and (3) include the following representations, made with respect to the two years prior to the date of the Cybersecurity Confirmation:

1. The EPN User or applicant has defined and maintains a comprehensive cybersecurity program and framework that considers potential cyber threats that impact their organization and protects the confidentiality, integrity and availability requirements of their systems and information.

2. The EPN User or applicant has implemented and maintains a written enterprise cybersecurity policy or policies approved by senior management or the organization's board of directors, and the organization's cybersecurity framework is in alignment with standard industry best practices and guidelines, as indicated on the form of Cybersecurity Confirmation.

3. If using a third party service provider or service bureau(s) to connect or transact business or to manage the connection with the Corporation, the EPN User or applicant has an appropriate program to (a) evaluate the cyber risks and impact of these third-parties, and (b) review the third-party assurance reports.

4. The cybersecurity program and framework protect the segment of the EPN User's or applicant's system that connects to and/or interacts with the Corporation.

5. The EPN User or applicant has in place an established process to remediate cyber issues identified to fulfill the EPN User's or applicant's regulatory and/or statutory requirements.

6. The cybersecurity program's and framework's risk processes are updated periodically based on a risk assessment or changes to technology, business, threat ecosystem, and/or regulatory environment.

7. **A comprehensive review of the EPN User's or applicant's cybersecurity program and framework has been conducted by one of the following:**

- **The EPN User or applicant, if that organization has filed and maintains a current Certification of Compliance with the Superintendent of the New York State Department of Financial Services pursuant to 23 NYCRR 500;**

- **A regulator who assesses the program against a designated cybersecurity framework or industry standard, including those that are listed on the form of the Cybersecurity Confirmation and in an Important Notice issued by the Corporation from time to time;**

- **An independent external entity with cybersecurity domain expertise, including those that are listed on the form of the Cybersecurity Confirmation and in an Important Notice issued by the Corporation from time to time; and**

- **An independent internal audit function reporting directly to the board of directors or designated board of directors committee of the EPN User or applicant, such that the findings of that review are shared with these governance bodies.**

* * *

ARTICLE III
EPN USERS

Rule 1. Requirements Applicable to EPN Users

* * *

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) has sufficient financial ability to meet its obligations to the Corporation; ~~**and**~~

(b) 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**

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

* * *

Sec. 8. General Continuance Standards

A. Ongoing Obligation to Notify the Corporation

An EPN User shall promptly inform the Corporation, both orally and in writing, if the EPN User is no longer in compliance with any of the requirements for admission to membership set forth in the EPN Rules. Notification must take place within two Business Days from the date on which the EPN User first learns of its non-compliance. In addition, an EPN User shall notify the Corporation within two Business Days of learning of an investigation or proceeding to which it is or is becoming subject that would cause the EPN User to fall out of compliance with any of the relevant requirements for membership set forth in the EPN Rules. Notwithstanding the previous sentence, the EPN User shall not be required to notify the Corporation if doing so would cause the EPN User to violate an applicable law, rule or regulation. If (a) the EPN User fails to maintain the relevant requirements for admission to membership, including but not limited to operational testing and related reporting requirements imposed by the Corporation from time to time; (b) the EPN User violates any EPN Rule or other agreement with the Corporation; (c) the EPN User fails to satisfy in a timely manner any obligation to the Corporation; (d) there is a Reportable Event

relating to such EPN User; or (e) the Corporation otherwise deems it necessary or advisable, in order to protect the Corporation, its other EPN Users, or its creditors or investors, to safeguard securities and funds in the custody or control of the Corporation, or to promote the prompt and accurate processing, clearance or settlement of securities transactions, the Corporation will undertake action to determine the status of the EPN User and its continued eligibility.

Furthermore, an EPN User must submit to the Corporation written notice of any Reportable Event at least 90 calendar days prior to the effective date of such Reportable Event unless the EPN User demonstrates that it could not have reasonably done so, and provided notice, both orally and in writing, to the Corporation as soon as possible.

In addition, if the Corporation has reason to believe that an EPN User may fail to comply with any of the EPN Rules, the Corporation may require the EPN User to provide it, within such timeframe, in such detail, and pursuant to such manner as the Corporation shall determine, with assurances in writing of a credible nature that the EPN User shall not, in fact, violate any of the EPN Rules.

B. Ongoing Obligation to Provide Cybersecurity Confirmation

As a condition to continued membership, EPN Users 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.

* * *