SECURITIES AND EXCHANGE COMMISSION
(Release No. 34-87697; File No. SR-FICC-2019-005)

December 9, 2019

Self-Regulatory Organizations; Fixed Income Clearing Corporation; Order Approving a Proposed Rule Change to Require Confirmation of Cybersecurity Program

I. Introduction

On October 15, 2019, FICC Clearing Corporation ("FICC") filed with the Securities and Exchange Commission ("Commission"), pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 ("Act")[1] and Rule 19b-4 thereunder,[2] proposed rule change SR-FICC-2019-005. The proposed rule change was published for comment in the Federal Register on October 30, 2019.[3] The Commission did not receive any comment letters on the proposed rule change. For the reasons discussed below, the Commission is approving the proposed rule change.

II. Description of the Proposed Rule Change

FICC proposes to modify its Government Securities Division ("GSD") Rulebook ("GSD Rules"), 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")[4] in order to

---

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

2 17 CFR 240.19b-4.

3 Securities Exchange Act Release No. 87394 (October 24, 2019), 84 FR 58194 (October 30, 2019) (SR-FICC-2019-005) ("Notice").

4 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 Order include the participants of GSD and MBSD, including GSD Netting Members, GSD Comparison-Only Members, GSD Sponsoring Members, GSD

(1) define the term "Cybersecurity Confirmation" as a written representation that addresses a submitting entity's cybersecurity program (described more fully below); and (2) require FICC's members and applicants for membership to submit to FICC a Cybersecurity Confirmation (both as part of an initial application for membership, and on an ongoing basis for members, at least every two years).

A. Background

FICC plays a prominent role in the fixed income markets as the sole clearing agency in the United States acting as a central counterparty and provider of significant clearance and settlement services for cash settled U.S. treasury and agency securities and the non-private label mortgage-backed securities markets.[5] In light of FICC's critical role in the marketplace, FICC was designated a Systemically Important Financial Market Utility ("SIFMU") under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.[6] Due to FICC's unique position in the marketplace, a failure or a disruption to FICC could, among other things, 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.[7]

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.

5 See Financial Stability Oversight Counsel 2012 Annual Report, Appendix A ("FSOC 2012 Report"), available at http://www.treasury.gov/initiatives/fsoc/Documents/2012%20Annual%20Report.pdf.

6 12 U.S.C. 5465(e)(1). See FSOC 2012 Report, supra note 5.

7 See FSOC 2012 Report, supra note 5.

FICC's members connect to FICC, either through the Securely Managed and Reliable Technology ("SMART") network or through other electronic means, such as a third party service provider, service bureau, network, or the Internet. 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. Currently, FICC does not require its members or applicants for membership to represent that they maintain a cybersecurity program as a condition for connecting to FICC via the SMART network or other means.

FICC states that many of its members and applicants for membership may currently be subject to regulations that are designed, in part, to protect against cyberattacks.[8] Accordingly, such entities would currently be required to follow standards established by national or international organizations focused on information security management, and they would currently maintain protocols for their senior management to verify the existence of cybersecurity programs sufficient to meet regulatory obligations. FICC further believes that some of its members and applicants for membership might also currently follow protocols substantially similar to the regulations referred to earlier

---

8 For example, depending on the type of entity, FICC states that its 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). Notice, supra note 3, at 58195.

in this paragraph in order to meet the evolving cybersecurity expectations of regulators and/or their own institutional customers.[9]

Although FICC believes that its members and applicants for membership may currently maintain robust cybersecurity programs, FICC seeks to better ensure the protection of its network by requiring its members and applicants for membership to confirm that they are meeting certain cybersecurity standards in order to connect to FICC via the SMART network or other means. Therefore, FICC proposes to require all members and applicants for membership to submit a written Cybersecurity Confirmation that includes specific representations regarding the submitting entity's cybersecurity program and framework. FICC states that the information contained in the Cybersecurity Confirmation would help FICC to better understand the cybersecurity programs and frameworks of entities seeking to connect to FICC, and thereby identify possible cyber risk exposures.[10] As a result, FICC would be better able to establish appropriate controls to mitigate such risks and their possible impacts on FICC's operations.

B. Proposed Changes

FICC proposes to modify its Rules to: (1) provide a detailed definition of the Cybersecurity Confirmation; and (2) require FICC's members and applicants for membership to submit to FICC a Cybersecurity Confirmation (both as part of an initial application for membership, and on an ongoing basis for members, at least every two years). Each of these proposed rule changes is described in greater detail below.

1. Cybersecurity Confirmation

---

9 Id.

10 Notice, supra note 3, at 58194-95.

FICC proposes to define the term "Cybersecurity Confirmation" to mean a written form, in a format provided by FICC and signed by the submitting entity's designated senior executive with the authority to attest to the cybersecurity matters contained in the form.[11] The form would contain specific representations regarding the submitting entity's cybersecurity program and framework. Such representations would cover the two years prior to the date of the most recently provided Cybersecurity Confirmation. The Cybersecurity Confirmation would include the following representations:

- The submitting entity has defined and maintains a comprehensive cybersecurity program and framework that considers potential cyber threats that impact the submitting entity's organization, and protects the confidentiality, integrity, and availability requirements of its systems and information.
- The submitting entity has implemented and maintains a written enterprise cybersecurity policy or policies approved by the submitting entity's senior management or board of directors, and the submitting entity's cybersecurity framework is in alignment with standard industry best practices and guidelines.[12]

---

11 Notice, supra note 3, at 58195. See also FICC Cybersecurity Confirmation Form, submitted as Exhibit 3 to SR-FICC-2019-005, available at https://www.sec.gov/rules/sro/ficc/2019/34-87394-ex3.pdf.

12 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,

- If the submitting entity uses a third party service provider or service bureau(s) to connect or transact business or to manage the connection with FICC, the submitting entity has an appropriate program to evaluate the cyber risks and impact of these third parties and to review the third party assurance reports.
- The submitting entity's cybersecurity program and framework protects the segment of its system that connects to and/or interacts with FICC.
- The submitting entity has in place an established process to remediate cyber issues identified to meet its regulatory and/or statutory requirements.
- The submitting entity periodically updates the risk processes of its cybersecurity program and framework based on a risk assessment or changes to technology, business, threat ecosystem, and/or regulatory environment.
- The submitting entity's cybersecurity program and framework has been reviewed by one of the following: (1) the submitting entity, 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

---

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. Notice, supra note 3, at 58195.

Services Companies;[13] (2) a regulator who assesses the submitting entity's cybersecurity program and framework against an industry cybersecurity framework or industry standard, including those that are listed on the Cybersecurity Confirmation form and in an Important Notice that is issued by FICC from time to time;[14] (3) an independent external entity with cybersecurity domain expertise in relevant industry standards and practices, including those that are listed on the Cybersecurity Confirmation form and in an Important Notice that is issued by FICC from time to time;[15] or (4) an independent internal audit function reporting directly to the submitting entity's board of directors or

---

13 23 N.Y. Comp. Codes R. & Regs. tit. 23, § 500 et seq. (2017). FICC states that this regulation requires entities to confirm that they have comprehensive cybersecurity programs as described in the regulation, and FICC believes this regime is sufficient to meet the objectives of the proposed Cybersecurity Confirmation. Notice, supra note 3, at 58196.

14 FICC states that current 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 Cybersecurity Confirmation form 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. Notice, supra note 3, at 58196.

15 FICC states that a third party with cybersecurity domain expertise is one that follows and understands applicable industry standards, practices, and regulations, such as ISO 27001 certification or NIST CSF assessment. FICC would identify acceptable industry standards and practices in the Cybersecurity Confirmation form 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. Notice, supra note 3, at 58196.

designated board of directors committee, such that the findings of that review are shared with these governance bodies.

FICC states that it designed the representations in the Cybersecurity Confirmation to provide information on how each submitting entity manages cybersecurity with respect to its connectivity to FICC.[16] FICC believes that by requiring these representations from members and applicants for membership, the proposed Cybersecurity Confirmation would provide useful information designed to enable FICC to make informed decisions about risks or threats, perform additional monitoring, target potential vulnerabilities, and otherwise protect the FICC network.[17]

2. Initial and Ongoing Membership Requirement

FICC proposes to require new applicants for FICC membership to submit a Cybersecurity Confirmation as part of their application materials. FICC also proposes to require all FICC members to submit a Cybersecurity Confirmation at least every two years. With respect to the requirement to submit a Cybersecurity Confirmation at least every two years, FICC would provide all members with notice of the date on which the Cybersecurity Confirmation would be due no later than 180 calendar days prior to the due date.

C. Implementation Timeframe

The proposed rule change would be effective upon Commission approval. New applicants for FICC membership would be required to submit a Cybersecurity Confirmation as part of their application materials. The requirement to submit a

---

16 Notice, supra note 3, at 58196.

17 Id.

Cybersecurity Confirmation would also apply to applicants whose applications are pending with FICC at the time the Commission approves the proposed rule change. For existing FICC members, FICC would provide notice of the due date to submit a Cybersecurity Confirmation, not later than 180 days prior to the due date. Finally, FICC would provide such notice to its members at least every two years going forward.

III. Discussion and Commission Findings

Section 19(b)(2)(C) of the Act[18] directs the Commission to approve a proposed rule change of a self-regulatory organization if it finds that such proposed rule change is consistent with the requirements of the Act and rules and regulations thereunder applicable to such organization. After carefully considering the proposed rule change, the Commission finds that the proposed rule change is consistent with the requirements of the Act and the rules and regulations thereunder applicable to FICC. In particular, the Commission finds that the proposed rule change is consistent with Section 17A(b)(3)(F) of the Act,[19] and Rules 17Ad-22(e)(17)(i) and (e)(17)(ii) promulgated under the Act,[20] for the reasons described below.

A. Consistency with Section 17A(b)(3)(F) of the Act

Section 17A(b)(3)(F) of the Act requires that the rules of a clearing agency be designed to, among other things, promote the prompt and accurate clearance and

---

18 15 U.S.C. 78s(b)(2)(C).

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

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

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.[21]

As described above, FICC proposes to require its members and applicants for membership to submit a Cybersecurity Confirmation, confirming the existence and nature of their cybersecurity programs. The Cybersecurity Confirmations should provide FICC with useful information regarding the cybersecurity programs of the submitting entities. By conditioning an entity's connectivity to FICC via the SMART network or other means on the submission of a Cybersecurity Confirmation, FICC should be better enabled to reduce the cyber risks of electronically connecting to entities that have not confirmed the existence and nature of their cybersecurity programs. Accordingly, the proposed Cybersecurity Confirmation requirement should provide FICC with information to better identify its exposure to cyber risks and to take steps to mitigate those risks.

If not adequately addressed, the risk of cyberattacks and other cyber vulnerabilities could affect FICC's network and 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. The proposed Cybersecurity Confirmation requirement is a tool designed to address those risks as described above. Therefore, the Commission finds the proposed Cybersecurity Confirmation requirement 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

---

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

or control of FICC or for which it is responsible, consistent with the requirements of Section 17A(b)(3)(F) of the Act.[22]

B. Consistency with Rule 17Ad-22(e)(17)(i) under the Act

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.[23] FICC's operational risks include protecting its electronic systems from cyber risks.

As described above, entities connect electronically to FICC via the SMART network or other means. The proposed Cybersecurity Confirmation requirement should reduce cyber risks to FICC by requiring members and applicants for membership to confirm that they have defined and maintain cybersecurity programs and frameworks that meet standard industry best practices and guidelines. The representations in each submitting entity's Cybersecurity Confirmation would provide information that should help FICC to mitigate its exposure to cyber risks, and thereby decrease the operational risks presented to FICC by its connections to such entities. Thus, the proposed Cybersecurity Confirmations should enable FICC to better identify potential sources of external operational risks and mitigate the possible impacts of those risks. Because the proposed changes would help FICC identify and mitigate plausible sources of external

---

22 Id.

23 17 CFR 240.17Ad-22(e)(17)(i).

operational risk, the Commission finds the proposed changes are consistent with the requirements of Rule 17Ad-22(e)(17)(i) under the Act.[24]

C. Consistency with Rule 17Ad-22(e)(17)(ii) under the Act

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.[25] As noted above, FICC's operational risks include protecting its electronic systems from cyber risks.

Although FICC believes that its members and applicants for membership may currently maintain robust cybersecurity programs, FICC currently does not require those entities to represent that they maintain a cybersecurity program as a condition for connecting to FICC via the SMART network or other means. FICC designed the proposed Cybersecurity Confirmation requirement to reduce cyber risks by requiring its members and applicants for membership to confirm that they have defined and maintain cybersecurity programs and frameworks that meet standard industry best practices and guidelines. The representations in each submitting entity's Cybersecurity Confirmation would provide more security for FICC's SMART network and other systems by providing FICC with information designed to help manage its cyber-related operational risks, which in turn, would enable FICC to take steps necessary to strengthen the security of its network to mitigate those risks. Since the proposal would enhance FICC's ability

---

24 Id.

25 17 CFR 240.17Ad-22(e)(17)(ii).

to ensure that its systems have a high degree of security, resiliency, and operational reliability, the Commission finds the proposed changes are consistent with the requirements of Rule 17Ad-22(e)(17)(ii) under the Act.[26]

IV. Conclusion

On the basis of the foregoing, the Commission finds that the proposed rule change is consistent with the requirements of the Act and, in particular, with the requirements of Section 17A of the Act[27] and the rules and regulations promulgated thereunder.

IT IS THEREFORE ORDERED, pursuant to Section 19(b)(2) of the Act[28] that proposed rule change SR-FICC-2019-005, be, and hereby is, APPROVED.[29]

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.[30]

Jill M. Peterson
Assistant Secretary

---

26 Id.

27 15 U.S.C. 78q-1.

28 15 U.S.C. 78s(b)(2).

29 In approving the proposed rule change, the Commission considered the proposals' impact on efficiency, competition, and capital formation. 15 U.S.C. 78c(f).

30 17 CFR 200.30-3(a)(12).