Required fields are shown with yellow backgrounds and asterisks.

Page 1 of * 33

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

File No. * SR 2022 - * 004
Amendment No. (req. for Amendments *)

Filing by The Depository Trust Company

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

Initial * ☑ Amendment * ☐ Withdrawal ☐

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

Pilot ☐

Extension of Time Period for Commission Action * ☐

Date Expires *

Rule

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

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

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

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

Exhibit 2 Sent As Paper Document ☐

Exhibit 3 Sent As Paper Document ☐

Description

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

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

Contact Information

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

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

Title * [redacted]

E-mail * RuleFilingAdmin@dtcc.com

Telephone * [redacted] Fax

Signature

Pursuant to the requirements of the Securities Exchange of 1934, The Depository Trust Company has duty caused this filing to be signed on its behalf by the undersigned thereunto duty authorized.

Date 05/11/2022

By [redacted]
(Name *)

(Title *) [redacted]

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

Date: 2022.05.11 13:56:34 -04'00'

Required fields are shown with yellow backgrounds and astericks.

SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

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

Form 19b-4 Information *

Add | Remove | View

Narrative - DTC Tech Upgrade Rule -

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

Exhibit 1 - Notice of Proposed Rule Change *

Add | Remove | View

Exhibit 1A - DTC Tech Upgrade Rule -

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

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

Add | Remove | View

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

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

Add | Remove | View

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

☐ Exhibit Sent As Paper Document

Exhibit 3 - Form, Report, or Questionnaire

Add | Remove | View

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

☐ Exhibit Sent As Paper Document

Exhibit 4 - Marked Copies

Add | Remove | View

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

Exhibit 5 - Proposed Rule Text

Add | Remove | View

Exhibit 5 - DTC Tech Upgrade Rule - F

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

Partial Amendment

Add | Remove | View

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

1. Text of the Proposed Rule Change

(a) The proposed rule change of The Depository Trust Company ("DTC") is annexed hereto as Exhibit 5 and consists of modifications to DTC's Rules, By-Laws and Organization Certificate ("Rules")[1] to revise certain provisions in the Rules relating to the requirement of applicants for DTC membership, Participants and Pledgees, (collectively, "Participants") of DTC, to require that each Participant upgrade its network technology, and communications technology or protocols to meet standards that DTC shall publish from time to time. Each of the proposed changes are described in greater detail below.

(b) Not applicable.

(c) Not applicable.

2. Procedures of the Self-Regulatory Organization

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

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

(a) Purpose

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

(i) Background of the Requirement

Currently, DTC does not require, either as part of its application for membership or as an ongoing membership requirement, any level or version for network technology, such as a web browser or other technology, or any level or version of communications technology or protocols, such as email encryption, secure messaging, or file transfers, that are being used to connect to or communicate with DTC. In the current environment, DTC maintains multiple network and communications methods and protocols, some either obsolete or many years older than the

---

[1] Capitalized terms not defined herein are defined in the Rules, available at https://dtcc.com/~/media/Files/Downloads/legal/rules/DTC_rules.pdf.

current standard in order to support Participants using these older technologies, which leaves communications between DTC and its Participants vulnerable to interception or the introduction of unknown entries, and requires DTC to expend additional resources, both in personnel and equipment, to maintain older communications channels. In addition, Participant's use of older technology delays the implementation by DTC to upgrade its internal systems, which, by doing so, risks losing connectivity with a number of Participants. Given DTC's critical role in the marketplace, this is a risk that needs to be addressed.

DTC believes that it should require current network technology, and current communication technology and protocol standards for Participants connecting to its network. For example, The National Institute of Standards and Technology or NIST[2] Special Publication 800-52 revision 2, specifies servers that support government-only applications shall be configured to use TLS[3] 1.2 and should be configured to use TLS 1.3 as well. These servers should not be configured to use TLS 1.1 and shall not use TLS 1.0, SSL 3.0, or SSL 2.0.[4] The Internet Engineer Task Force ("IETF")[5] formally deprecated TLS versions 1.0 and 1.1 in March of 2021, stating, "These versions lack support for current and recommended cryptographic algorithms and mechanisms, and various government and industry profiles of applications using TLS now mandate avoiding these old TLS versions. … Removing support for older versions from implementations reduces the attack surface, reduces opportunity for misconfiguration, and streamlines library and product maintenance."[6] TLS 1.0 (published in 1999) does not support many modern, strong cipher (encryption) suites and TLS 1.1 (published in 2006) is a security improvement over TLS 1.0 but still does not support certain stronger cipher or encryption suites.[7] Another communications technology, File Transfer Protocol ("FTP") is considered an insecure protocol, because it transfers user authentication data (username and password) and file data as plain-text (not encrypted) over the network. This makes it highly vulnerable to sniffing attacks that allow an attacker to collect usernames and passwords from the network and inject malware into downloads via FTP. Following the guidance from NIST and other standards

---

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

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

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

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

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

7 Id.

organizations, the proposed change would require the use of TLS 1.2, Secure FTP ("SFTP"), along with other modern technology and communication standards and protocols to communication with Participants.

(ii) Proposed Rule Changes

To implement the proposed changes DTC would revise Rule 2, Section 11 to add the requirement that applicants for membership confirm their network technology, and communications technology and protocols to be at the levels specified by DTC, as part of their application. Rule 2, Section 11 would also be amended to add the requirement that each Participant or Pledgee maintain or upgrade their network technology, or communications technology, or protocols on the systems that connect to DTC to the version being required and within the time periods as provided through the Important Notice mechanism on the DTC website. Rule 21 would be updated to provide that a Participant or Pledgee who fails to perform the upgrade to their network technology, or communications technology, or protocols and in the required timeframe would be subject to the disciplinary sanctions, as specified in the Rules.

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

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

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

(b) Statutory Basis

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

---

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

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

(23)[10], promulgated under the Act as discussed below.

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

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

DTC believes that the proposed rule change requiring Participants to meet DTC's standards for network technology, or communications technology or protocols is consistent with this provision of the Act. By conditioning an entity's application to DTC on its use of DTC's current network technology and communications technology or protocols, DTC should be better enabled to reduce the cyber risks of electronically connecting to entities by reducing the risks of communication interception. Accordingly, the proposed requirement would allow DTC to reduce both DTC's and its Participant's exposure to interception or the introduction of malware while communicating between the entities. Intercepting communications or the introduction of malware or altered data could potentially compromise DTC's ability to promptly and accurately settle securities transactions and safeguard securities funds. The proposal is designed to mitigate those risks and thereby promote the prompt and accurate clearance and settlement of securities transactions, to assure the safeguarding of securities and funds which are in the custody or control of DTC or for which it is responsible and to remove impediments to and perfect the mechanism of a national system for the prompt and accurate clearance and settlement of securities transactions. Providing a clear and consistent standard at the current level of network and communication security and technology would allow Participants to better understand their obligations with respect to such technology and communication requirements and providing a uniform obligation for Participants with respect to such requirements. As such, DTC believes the proposed rule change is consistent with Section 17A(b)(3)(F) of the Act.[12]

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

In addition, the proposed rule change is designed to be consistent with Rule 17Ad 22(e)(21)(iv) promulgated under the Act. Rule 17Ad-22(e)(21)(iv) requires DTC to, inter alia, establish, implement, maintain and enforce written policies and procedures reasonably designed to be efficient and effective in meeting the requirements of its Participants and the markets it serves with regard to the use of network technology and communication technologies or protocols. The proposed rule change would enhance DTC's security through the use of current network technology, or communication technology or protocols, and would allow DTC to reduce its and its Participants' exposure to interception or the introduction of malware while communicating between the entities. This would eliminate the current use of multiple

---

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

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

12 Id.

generations of network technology and communications technology and protocols, including ones that NIST no longer permits for use on government systems due to their insecurity. The proposed rule would require, after appropriate notice to Participants, future network technology and communication or protocol upgrades as technology and threats evolve to maintain secure connectivity.

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

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

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

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

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

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

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

---

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

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

15 Id.

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

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

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

Rule 17Ad-22(e)(22)

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

The requirement to use industry approved communications technology or protocols, including those that NIST specifies as acceptable for use in government systems is a cornerstone of the changes being proposed by DTC. The use of older, obsolete, or insecure network technology or communications technology or protocols, including those specified to not be used by the IETF[19] represents a risk to efficient payment, clearing and settlement.

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

Rule 17Ad-22(e)(23)

The proposed rule change is also designed to be consistent with Rule 17Ad 22(e)(23)(i), (ii) and (iv) promulgated under the Act, which requires DTC to publicly disclose all relevant rules and material procedures, provide sufficient information to enable Participants to identify

---

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

17 Id.

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

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

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

and evaluate the risks, fees, potential monetary fines, and other material costs they incur by participating in the covered clearing agency, and to provide a comprehensive public disclosure that describes DTC's material rules, policies, and procedures regarding DTC's legal, governance, risk management and operating framework.[21]

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

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

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

DTC does not believe the proposed changes to require Participants to have, or to upgrade their network technology or communications technology or protocols would have any impact, or impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act.[23] Although the addition of the requirement to upgrade to current network technology or communications technology or protocols would be adding obligations on Participants with respect to how they communicate with DTC, such obligations would be reasonable because the requirements to protect client and customer data would allow DTC to reduce both its and its Participants' exposure to interception or the introduction of malware while communicating between the entities.

DTC believes that the proposed change described herein is necessary in furtherance of the purposes of Section 17A(b)(3)(F) of the Act,[24] and Rules 17Ad-22(e)(17), (e)(21), (e)(22), and (e)(23).[25] The proposed changes to require Participants to upgrade their network technology, and communications technology or protocols, will (i) allow DTC to protect it and its Participants and would promote the prompt and accurate clearance and settlement of securities consistent with the requirements of Section 17A(b)(3)(F) of the Act,[26] (ii) identify potential

---

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

22 Id.

23 15 U.S.C. 78q–1(b)(3)(I).

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

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

26 Id.

operational risks from the use of obsolete and insecure network technology and communications technology or protocols consistent with Rule 17Ad 22(e)(17)(i),[27] (iii) through the requirement of the use of current network technology and communications technology or protocols, ensure that systems have a high degree of security, resiliency, operational reliability, and adequate, scalable capacity, consistent with Rule 17Ad 22(e)(17)(ii),[28] and (iv) through the use of requiring relevant internationally accepted communication procedures and standards, facilitate efficient payment, clearing, and settlement, consistent with Rules 17Ad-22(e)(22).[29]

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

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

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

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

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

All prospective commenters should follow the SEC's instructions on how to submit comments, available at https://www.sec.gov/regulatory-actions/how-to-submit-comments. General questions regarding the rule filing process or logistical questions regarding this filing

---

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

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

29 Id.

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

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

should be directed to the Main Office of the SEC's Division of Trading and Markets at tradingandmarkets@sec.gov or 202-551-5777.

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

6. Extension of Time Period for Commission Action

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

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

(a) Not applicable.

(b) Not applicable.

(c) Not applicable.

(d) Not applicable.

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

While the proposal is not based on the rules of another self-regulatory organization or of the Commission, DTC's affiliates, Fixed Income Clearing Corporation and National Securities Clearing Corporation, 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 Notice Filed Pursuant to Section 806(e) of the Payment, Clearing, and Settlement Supervision Act of 2010

Not applicable.

11. Exhibits

Exhibit 1 – Not applicable.

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

Exhibit 2 – Not applicable.

---

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

Exhibit 3 – Not applicable.

Exhibit 4 – Not applicable.

Exhibit 5 – Proposed changes to the Rules.

EXHIBIT 1A

SECURITIES AND EXCHANGE COMMISSION
(Release No. 34-[_____]; File No. SR-DTC-2022-004)

[DATE]

Self-Regulatory Organizations; The Depository Trust Company; Notice of Filing of a Proposed Rule Change to Require Applicants and Members to Maintain or Upgrade Their Network or Communications Technology

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

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

The proposed rule change of DTC consists of modifications to Rules[3] to revise certain provisions in the Rules relating to the requirement of applicants for DTC membership, Participants and Pledgees, (collectively, "Participants") of DTC, to require that each Participant upgrade its network technology, and communications technology or protocols to meet standards that DTC shall publish from time to time, as described in greater detail below.

---

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 https://dtcc.com/~/media/Files/Downloads/legal/rules/DTC_rules.pdf.

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

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

(i) Background of the Requirement

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

DTC believes that it should require current network technology, and current communication technology and protocol standards for Participants connecting to its network. For example, The National Institute of Standards and Technology or NIST[4] Special Publication 800-52 revision 2, specifies servers that support government-only

---

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

applications shall be configured to use TLS[5] 1.2 and should be configured to use TLS 1.3 as well. These servers should not be configured to use TLS 1.1 and shall not use TLS 1.0, SSL 3.0, or SSL 2.0.[6] The Internet Engineer Task Force ("IETF")[7] formally deprecated TLS versions 1.0 and 1.1 in March of 2021, stating, "These versions lack support for current and recommended cryptographic algorithms and mechanisms, and various government and industry profiles of applications using TLS now mandate avoiding these old TLS versions. … Removing support for older versions from implementations reduces the attack surface, reduces opportunity for misconfiguration, and streamlines library and product maintenance."[8] TLS 1.0 (published in 1999) does not support many modern, strong cipher (encryption) suites and TLS 1.1 (published in 2006) is a security improvement over TLS 1.0 but still does not support certain stronger cipher or encryption suites.[9] Another communications technology, File Transfer Protocol ("FTP") is considered an insecure protocol, because it transfers user authentication data (username and password) and file data as plain-text (not encrypted) over the network.

---

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

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

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

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

9 Id.

This makes it highly vulnerable to sniffing attacks that allow an attacker to collect usernames and passwords from the network and inject malware into downloads via FTP. Following the guidance from NIST and other standards organizations, the proposed change would require the use of TLS 1.2, Secure FTP ("SFTP"), along with other modern technology and communication standards and protocols to communication with Participants.

(ii) Proposed Rule Changes

To implement the proposed changes DTC would revise Rule 2, Section 11 to add the requirement that applicants for membership confirm their network technology, and communications technology and protocols to be at the levels specified by DTC, as part of their application. Rule 2, Section 11 would also be amended to add the requirement that each Participant or Pledgee maintain or upgrade their network technology, or communications technology, or protocols on the systems that connect to DTC to the version being required and within the time periods as provided through the Important Notice mechanism on the DTC website. Rule 21 would be updated to provide that a Participant or Pledgee who fails to perform the upgrade to their network technology, or communications technology, or protocols and in the required timeframe would be subject to the disciplinary sanctions as specified in the Rules.

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

In order to provide Participants and Pledgees adequate time to complete a required network technology, or communications technology or protocol upgrade, the time for a Participant or Pledgee to complete a required upgrade shall be set forth in the form of a notice posted on DTC's website, with the timeline determined for the due date of any upgrade. DTC maintains a security policy and control standards that include a

review of industry, vendor and U.S. Government best practice guidelines and timelines for security reviews which are used to determine whether an upgrade may be required. Due dates for an upgrade shall be published on the website based on DTC's reasonable estimates of the complexity or potential cost of an upgrade, an estimate of potential licensing fees, an estimate of the resources that may be needed to support an upgrade, or the urgency to remediate published vulnerabilities.

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

2. Statutory Basis

DTC believes that the proposal is consistent with the requirements of the Act[10] and the rules and regulations thereunder applicable to a registered clearing agency. In particular, DTC believes that the proposed rule changes is consistent with Section 17A(b)(3)(F) of the Act,[11] and Rules 17Ad-22(e)(17)(i) and (ii), (21), (23)[12], promulgated under the Act as discussed below.

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

Section 17A(b)(3)(F) of the Act[13] requires, in part, that the Rules be designed to promote the prompt and accurate clearance and settlement of securities transactions, to

---

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

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

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

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

assure the safeguarding of securities and funds which are in the custody or control of DTC or for which it is responsible and to remove impediments to and perfect the mechanism of a national system for the prompt and accurate clearance and settlement of securities transactions.

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

respect to such requirements. As such, DTC believes the proposed rule change is consistent with Section 17A(b)(3)(F) of the Act.[14]

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

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

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

---

14 Id.

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

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

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

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

---

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

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

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

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

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

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

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

Rule 17Ad-22(e)(22)

---

17 Id.

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

19 Id.

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

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

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

Rule 17Ad-22(e)(23)

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

---

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

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

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

and procedures regarding DTC's legal, governance, risk management and operating framework.[23]

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

Therefore, by providing Participants with public and readily available access to the required network technology, or communications technology or protocols, DTC believes that the proposed change is consistent with the requirements of Rule 17Ad-22(e)(23)(i)(ii) and (iv), promulgated under the Act.[24]

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

DTC does not believe the proposed changes to require Participants to have, or to upgrade their network technology or communications technology or protocols would have any impact, or impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act.[25] Although the addition of the requirement to upgrade to current network technology or communications technology or protocols would be adding obligations on Participants with respect to how they communicate with DTC, such obligations would be reasonable because the requirements to protect client and

---

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

24 Id.

25 15 U.S.C. 78q–1(b)(3)(I).

customer data would allow DTC to reduce both its and its Participants' exposure to interception or the introduction of malware while communicating between the entities.

DTC believes that the proposed change described herein is necessary in furtherance of the purposes of Section 17A(b)(3)(F) of the Act,[26] and Rules 17Ad-22(e)(17), (e)(21), (e)(22), and (e)(23).[27] The proposed changes to require Participants to upgrade their network technology, and communications technology or protocols, will (i) allow DTC to protect it and its Participants and would promote the prompt and accurate clearance and settlement of securities consistent with the requirements of Section 17A(b)(3)(F) of the Act,[28] (ii) identify potential operational risks from the use of obsolete and insecure network technology and communications technology or protocols consistent with Rule 17Ad 22(e)(17)(i),[29] (iii) through the requirement of the use of current network technology and communications technology or protocols, ensure that systems have a high degree of security, resiliency, operational reliability, and adequate, scalable capacity, consistent with Rule 17Ad 22(e)(17)(ii),[30] and (iv) through the use of requiring relevant internationally accepted communication procedures and standards, facilitate efficient payment, clearing, and settlement, consistent with Rules 17Ad-22(e)(22).[31]

---

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

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

28 Id.

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

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

31 Id.

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

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

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

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

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

---

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

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

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

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

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

Within 45 days of the date of publication of this notice in the Federal Register or within such longer period up to 90 days (i) as the Commission may designate if it finds such longer period to be appropriate and publishes its reasons for so finding or (ii) as to which the self-regulatory organization consents, the Commission will:

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

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

IV. Solicitation of Comments

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

Electronic Comments:

- Use the Commission's Internet comment form (http://www.sec.gov/rules/sro.shtml); or
- Send an e-mail to rule-comments@sec.gov. Please include File Number SR-DTC-2022-004 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-DTC-2022-004. 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 DTC 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-DTC-2022-004 and should be submitted on or before [insert date 21 days from publication in the Federal Register].

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

Secretary

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

EXHIBIT 5

Bold and underlined text indicates proposed added language

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

RULES

BY-LAWS

ORGANIZATION CERTIFICATE

THE DEPOSITORY TRUST COMPANY

RULE 2

PARTICIPANTS AND PLEDGEES

* * *

Section 11. As part of their application materials, each applicant to become a Participant or Pledgee shall complete and deliver to the Corporation a Cybersecurity Confirmation (as defined below)**, in addition to the successful completion of network and connectivity testing at the current DTC standards (the scope of such testing to be determined by the Corporation in its sole discretion).**

Each Participant and Pledgee 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.

The term "Cybersecurity Confirmation" means a written document provided to the Corporation by all Participants, Pledgees 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 Participant, Pledgee 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 Participant, Pledgee 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 Participant, Pledgee 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 Participant, Pledgee 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 Participant's, Pledgee's or applicant's system that connects to and/or interacts with the Corporation.

5. The Participant, Pledgee or applicant has in place an established process to remediate cyber issues identified to fulfill the Participant's, Pledgee'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 Participant's, Pledgee's or applicant's cybersecurity program and framework has been conducted by one of the following:

   - The Participant, Pledgee 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 Participant, Pledgee or applicant, such that the findings of that review are shared with these governance bodies.

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

RULE 21

DISCIPLINARY SANCTIONS

The Corporation may discipline a Participant or Pledgee for a violation of these Rules or the Procedures or for errors, delays or other conduct detrimental to the operations of the Corporation, other Participants or Pledgees, or for not providing adequate facilities for its business with the Corporation**, or failure to perform the upgrade to their network technology, or communications technology or protocols as required under these Rules in the time specified,** by imposing any of the following sanctions: expulsion; suspension; limitation of activities, functions and operations; fine; censure; and any other fitting sanction. In addition, in the event that a Participant shall violate these Rules, the Procedures or any of its agreements with the Corporation, the Corporation may require such cash or other deposit by a Participant to the Participants Fund or otherwise as shall be necessary or appropriate to protect the Corporation, other Participants or Pledgees, in the circumstances.

In the event that a Participant shall fail to settle, the Corporation is authorized by these Rules and the Procedures to charge interest to that Participant and/or other Participants in substantially the same amounts as the Corporation shall have paid by reason of such event; the charge of such interest shall not be considered a disciplinary sanction subject to this Rule or Rule 22.

When the Corporation proposes to impose a sanction it shall send the Participant or Pledgee a written statement describing the reason for the proposed sanction and notifying the Participant or Pledgee that it has an opportunity to respond pursuant to Rule 22. The sanction proposed may be imposed by the Chairman of the Board, the President or the Secretary unless, within five Business Days after notification of such proposed sanction, the Participant or Pledgee provides notice of its desire to contest the sanction, as provided in Rule 22. The right to contest a sanction before it is imposed pursuant to Rule 22 shall not apply to a case where the Corporation summarily suspends and closes the accounts of a Participant or Pledgee pursuant to the Exchange Act.

> *Note*: Section 17A(b)(5)(C) of the Exchange Act permits the Corporation summarily to suspend and close the Accounts of a Participant. That section also provides that a Participant so summarily suspended shall be promptly afforded an opportunity for hearing by the Corporation and that the appropriate regulatory agency for the Participant may stay any such summary suspension. Section 19 of the Exchange Act contains provisions relevant to a Participant's remedies in the event of its summary suspension..