

SECURITIES AND EXCHANGE COMMISSION
(Release No. 34-95232; File No. SR-DTC-2022-004)

July 8, 2022

Self-Regulatory Organizations; The Depository Trust Company; Order Approving a Proposed Rule Change to Require Applicants, Participants, and Pledges to Maintain or Upgrade Their Network or Communications Technology

I. INTRODUCTION

On May 11, 2022, The Depository Trust Company (“DTC”) filed with the Securities and Exchange Commission (“Commission”) proposed rule change SR-DTC-2022-004 (“Proposed Rule Change”) pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 (“Act”)¹ and Rule 19b-4 thereunder.² The Proposed Rule Change was published for comment in the Federal Register on May 31, 2022.³ 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

A. Background

DTC proposes to modify its Rules (“Rules”)⁴ to require its Participants, Pledges, and applicants for membership (collectively, “participants”) to upgrade and maintain their network technology, and communications technology or protocols, to meet

¹ 15 U.S.C. 78s(b)(1).

² 17 CFR 240.19b-4.

³ Securities Exchange Act Release No. 94975 (May 24, 2022), 87 Fed. Reg. 32482 (May 31, 2022) (SR-DTC-2022-004) (“Notice of Filing”).

⁴ DTC’s Rules are available at https://dtcc.com/~media/Files/Downloads/legal/rules/dtc_rules.pdf.

standards that DTC would identify and publish via Important Notice on its website, as described more fully below.

DTC provides depository services and asset servicing for a wide range of security types such as money market instruments, equities, warrants, rights, corporate debt and notes, municipal bonds, government securities, asset-backed securities, and collateralized mortgage obligations.⁵ In light of its critical role in the marketplace, DTC 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 DTC’s unique position in the marketplace, a failure or a disruption at DTC 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

DTC’s Rules currently do not require, either as part of an 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 participants may use to connect to or communicate with DTC.⁸

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, Appendix A, supra note 5.

⁸ Notice of Filing, supra note 3, at 32482.

Therefore, DTC currently maintains multiple network and communications methods and protocols to interact with its participants.⁹ This includes some outdated communication technologies in order to support participants that continue to use such older technologies.¹⁰ DTC believes that continuing to use such outdated technologies could render communications between DTC and some of its participants vulnerable to cyber risks.¹¹ Additionally, participants' use of outdated technology delays DTC's implementation of its own internal system upgrades, which by doing so, risks losing connectivity between DTC and a number of its participants.¹² Finally, DTC states that it currently expends additional resources, both in personnel and equipment, to maintain outdated communications channels.¹³

To mitigate the foregoing security concerns and resource inefficiencies, DTC proposes to require its participants to upgrade and maintain network technology, communication technology, and protocol standards, in accordance with applicable technology standards that DTC would identify and publish via Important Notice on its website from time to time.¹⁴ DTC would base these requirements on standards set forth by widely accepted organizations such as the National Institute of Standards and

⁹ Id.

¹⁰ Id.

¹¹ Id.

¹² Id.

¹³ Id.

¹⁴ Id., at 32482-83.

Technology (“NIST”) and the Internet Engineer Task Force (“IETF”).¹⁵

To implement the proposed changes, DTC would revise its Rules to require participants to maintain or upgrade their network technology, communications technology, or protocols on the systems that connect to DTC, to the version DTC requires, within the time period DTC requires.¹⁶ Consistent with the guidance from NIST and other standards organizations, DTC would require the use of TLS 1.2, Secure FTP (“SFTP”), and other modern technology and communication standards and protocols, by its participants for communication with DTC.¹⁷ DTC would publish such requirements

¹⁵ Id. NIST is part of the U.S. Department of Commerce. The IETF is an open standards organization that develops and promotes voluntary Internet standards, in particular, the technical standards that comprise the Internet protocol suite (TCP/IP). For example, NIST Special Publication 800-52 revision 2, specifies servers that support government-only applications shall be configured to use Transport Layer Security (“TLS”) 1.2 and should be configured to use TLS 1.3 as well. See <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf>. (TLS, the successor of the now-deprecated Secure Sockets Layer (“SSL”), is a cryptographic protocol designed to provide communications security over a computer network.) 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. Additionally, the IETF formally deprecated TLS versions 1.0 and 1.1 in March of 2021, stating that “[t]hese 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.” See <https://datatracker.ietf.org/doc/rfc8996/>. DTC would also require participants to discontinue using File Transfer Protocol (“FTP”), which DTC believes to be an insecure protocol because it transfers user authentication data (username and password) and file data as plain-text (not encrypted) over the network. Notice of Filing, supra note 3, at 32482-83.

¹⁶ Notice of Filing, supra note 3, at 32483.

¹⁷ Id., at 32482-83.

via Important Notice on its website.¹⁸ DTC also proposes to amend its Rules to provide that failure to perform a necessary technology upgrade within the required timeframe would subject participants to a disciplinary sanctions.¹⁹

III. DISCUSSION AND COMMISSION FINDINGS

Section 19(b)(2)(C) of the Act²⁰ 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 the rules and regulations thereunder applicable to such organization. After careful consideration, the Commission finds that the Proposed Rule Change is consistent with the requirements of the Act and the rules and regulations applicable to DTC. In particular, the Commission finds that the Proposed Rule Change is consistent with Sections 17A(b)(3)(F)²¹ and (b)(3)(G)²² of the Act and Rules 17Ad-22(e)(17)²³ and (e)(21)²⁴ thereunder.

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 settlement of securities transactions and assure the safeguarding of securities and funds

¹⁸ Id.

¹⁹ Notice of Filing, supra note 3, at 32483.

²⁰ 15 U.S.C. 78s(b)(2)(C).

²¹ 15 U.S.C. 78q-1(b)(3)(F).

²² 15 U.S.C. 78q-1(b)(3)(G).

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

²⁴ 17 CFR 240.17Ad-22(e)(21)(iv).

which are in the custody or control of the clearing agency or for which it is responsible.²⁵

As described above, DTC proposes to require its participants to upgrade and maintain network technology, and communication technology and protocol standards, that meet the standards identified by DTC and published via Important Notice to DTC's website from time to time. DTC would use standards set forth by widely accepted organizations such as NIST and the IETF as the requirements. The proposed requirements would enable DTC to avoid communicating with its participants using outdated technologies that present security vulnerabilities to DTC. Specifically, as an initial matter, the proposed requirements would enable DTC to discontinue using communication technologies such as TLS 1.0, TLS 1.1, SSL 2.0, SSL 3.0, and FTP, which have been deemed not secure by organizations such as NIST and/or the IETF. Removing support for such outdated technologies would reduce DTC's potential exposure to cyberattacks and other cyber vulnerabilities.

If not adequately addressed, the risk of cyberattacks and other cyber vulnerabilities could affect DTC's network and, in turn, DTC's ability to clear and settle securities transactions, or to safeguard the securities and funds which are in DTC's custody or control, or for which it is responsible. DTC designed the proposed requirements for participants to upgrade their communications technology to address those risks, as described above. Accordingly, the Commission finds the proposed technology requirements on DTC's participants 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 DTC or for which it is

²⁵ 15 U.S.C. 78q-1(b)(3)(F).

responsible, consistent with the requirements of Section 17A(b)(3)(F) of the Act.²⁶

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

Section 17A(b)(3)(G) of the Act requires the rules of a clearing agency to provide that its participants shall be appropriately disciplined for violation of any provision of the rules of the clearing agency by fine or other fitting sanction.²⁷ As noted above, DTC proposes to require its participants to upgrade and maintain network technology, communication technology, and protocol standards, in accordance with applicable technology standards that DTC would identify and publish via Important Notice on its website. The proposed requirements would enable DTC to avoid communicating with its participants using outdated technologies that present security vulnerabilities to DTC. If not adequately addressed, such vulnerabilities could affect DTC's network and its ability to operate. DTC also proposes to amend its Rules to provide that failure to perform a necessary technology upgrade within the required timeframe would subject participants to disciplinary sanctions. Because the proposed disciplinary sanctions should incentivize DTC's participants to upgrade and maintain secure communications technology, thereby reducing DTC's operational risks, the Commission finds the proposed rule change is consistent with the requirements of Section 17A(b)(3)(G) of the Act.²⁸

²⁶ Id.

²⁷ 15 U.S.C. 78q-1(b)(3)(G).

²⁸ Id. Additionally, by including the monetary fine provision in its Rules, DTC would enable its participants to better identify and evaluate the material costs they might incur by participating in DTC, consistent with Rule 17Ad-22(e)(23)(ii) under the Act, which requires a covered clearing agency to establish, implement, maintain, and enforce written policies and procedures reasonably designed to provide sufficient information to enable participants to identify and evaluate the

C. Consistency with Rule 17Ad-22(e)(17) 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.²⁹ DTC's operational risks include cyber risks to its electronic systems.

As described above, DTC and its participants connect electronically to communicate with one another. However, DTC's Rules currently do not require 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 participants may use to connect to or communicate with DTC. As a result, DTC maintains some outdated communication technologies in order to support participants that continue to use such older technologies. Continuing to use such outdated technologies could render communications between DTC and some of its participants vulnerable to cyber risks.

To mitigate the foregoing cyber risks, DTC proposes to require its participants to upgrade and maintain network technology, and communication technology and protocol standards that meet the standards identified by DTC from time to time. The proposed technology requirements should reduce DTC's cyber risk by requiring participants to

risks, fees, and other material costs they incur by participating in the covered clearing agency. See 17 CFR 240.17Ad-22(e)(23)(ii).

²⁹ 17 CFR 240.17Ad-22(e)(17)(i).

upgrade and maintain communications technology based on standards set forth by widely accepted organizations such as NIST and the IETF, thereby decreasing the operational risks presented to DTC. Because the proposed technology requirements would help DTC mitigate plausible sources of external operational risk, the Commission finds the proposed changes are consistent with the requirements of Rule 17Ad-22(e)(17)(i) under the Act.³⁰

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.³¹ As noted above, DTC's operational risks include cyber risks.

As described above, DTC's Rules currently do not require 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 participants may use to connect to or communicate with DTC. DTC designed the proposed technology requirements to reduce cyber risks by requiring its participants to upgrade and maintain communications technology based on standards set forth by widely accepted organizations such as NIST and the IETF. Requiring DTC's participants to use only secure communications technology would reduce DTC's cyber risks and thereby strengthen the security, resiliency, and operational reliability of DTC's network and other systems. Because the proposed technology requirements would

³⁰ Id.

³¹ 17 CFR 240.17Ad-22(e)(17)(ii).

enhance DTC's ability to ensure that its systems have a high degree of security, resiliency, and operational reliability, the Commission finds the Proposed Rule Change is consistent with the requirements of Rule 17Ad-22(e)(17)(ii) under the Act.³²

D. Consistency with Rule 17Ad-22(e)(21) Under the Act

Rule 17Ad-22(e)(21)(iv) under the Act requires that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to have the covered clearing agency's management regularly review the efficiency and effectiveness of its use of technology and communication procedures.³³

As mentioned above, DTC maintains multiple network and communication methods to interact with its participants, including certain outdated communication technologies necessary to support participants that continue to use such older technologies. DTC believes that continuing to use such outdated technologies could render communications between DTC and some of its participants vulnerable to cyber risks. Additionally, participants' use of outdated technology delays DTC's implementation of its own internal system upgrades, which by doing so, risks losing connectivity between DTC and a number of its participants. Finally, DTC states that it currently expends unnecessary resources to maintain outdated communications channels. In other words, DTC has subjected its network communication methods to review for efficiency and effectiveness. As a result, to enhance the efficiency and effectiveness of its technology and communication procedures, DTC proposes to require its participants to upgrade and maintain network technology, communication technology, and protocol

³² Id.

³³ 17 CFR 240.17Ad-22(e)(21)(iv).

standards, in accordance with applicable technology standards that DTC would identify and publish via Important Notice on its website. Because the Proposed Rule Change is an outgrowth of DTC’s review of the efficiency and effectiveness of its technology and communication procedures, the Commission finds the Proposed Rule Change is consistent with the requirements of Rule 17Ad-22(e)(21)(iv) under the Act.³⁴

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 Act³⁵ and the rules and regulations promulgated thereunder.

IT IS THEREFORE ORDERED, pursuant to Section 19(b)(2) of the Act³⁶ that Proposed Rule Change SR-DTC-2022-004, be, and hereby is, APPROVED.³⁷

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.³⁸

J. Matthew DeLesDernier,
Assistant Secretary.

³⁴ Id.

³⁵ 15 U.S.C. 78q-1.

³⁶ 15 U.S.C. 78s(b)(2).

³⁷ In approving the Proposed Rule Change, the Commission considered the proposals’ impact on efficiency, competition, and capital formation. 15 U.S.C. 78c(f).

³⁸ 17 CFR 200.30-3(a)(12).