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..