EXHIBIT 5

Bold and underlined text indicates proposed added language.

RULES, BY-LAWS AND ORGANIZATION CERTIFICATE

OF 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).

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.**

***