EXHIBIT A

OCC Rules

Underlined text indicates new text

~~Strikethrough~~ text indicates deleted text

RULE 213~~9~~ – Cybersecurity ~~Confirmation~~ Obligations

(a) *Cybersecurity Confirmation Submission.* Each Clearing Member and applicant for clearing membership shall complete and submit a form, provided by the Corporation, that confirms the existence of an information system cybersecurity program and includes required representations as determined by the Corporation ("Cybersecurity Confirmation").

(i) Each applicant for clearing membership shall submit a completed Cybersecurity Confirmation as part of its application materials.

(ii) Each Clearing Member shall submit a completed Cybersecurity Confirmation at least every two years and not later than 180 calendar days from the date that ~~OCC~~the Corporation notifies the Clearing Member that an attestation is required.

(b) *Representations in the Cybersecurity Confirmation.* The Cybersecurity Confirmation shall consist of representations including, but not limited to, the following:

(1) The Clearing Member or applicant for clearing membership 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 Clearing Member or applicant for clearing membership 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. ~~OCC~~The Corporation may consider requests to recognize additional best practices and guidelines that are not 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 Clearing Member or applicant for clearing membership 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 Clearing Member's or applicant's system that connects to and/or interacts with the Corporation.

(5) The Clearing Member or applicant has in place an established process to remediate cyber issues identified to fulfill the Clearing Member'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 Clearing Member's or applicant's cybersecurity program and framework has been conducted by one of the following:

- The Clearing Member 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 Information Memorandum published 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 Information Memorandum published 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 Clearing Member or applicant, such that the findings of that review are shared with these governance bodies.

(c) *Execution of the Cybersecurity Confirmation.* The Cybersecurity Confirmation shall be signed by a designated senior executive of the Clearing Member or applicant who is authorized to attest to these matters.

(d) *Occurrence of a Security Incident.* A Clearing Member must notify the Corporation immediately, and shall promptly confirm such notice in writing, if the Clearing Member becomes aware or should be aware that there has been an incident, or an incident is occurring, involving a cyber-related disruption or intrusion of the Clearing Member's system(s) that is reasonably likely to pose an imminent risk or threat to the Corporation's operations. Such occurrence may include, but is not limited to, any disruption or degradation of the normal operation of the Clearing Member's system(s) or any unauthorized entry into the Clearing Member's system(s) that would result in loss of the Corporation's data or system integrity, unauthorized disclosure of sensitive information related to the Corporation, or the inability of the Corporation to conduct essential clearance and settlement functions ("Security Incident"). Upon such notice, or if the Corporation has a reasonable basis to believe that a Security Incident has occurred, or is occurring, the Corporation may take actions reasonably necessary to mitigate any effects to its operations, including the right to disconnect access, or to modify the scope and specifications of access, of the Clearing Member to the Corporation's information and data systems. In determining whether to disconnect a Clearing Member, the Corporation will evaluate the facts and circumstances related to the Security Incident. The Corporation may take into consideration a number of factors, including, but not limited to, the potential loss of control by a Clearing Member of its internal system(s), the potential loss of the Corporation's confidential data, the potential strain on or loss of the Corporation's resources due to the Corporation's inability to perform clearance and settlement functions, and the overall severity of the threat to the security and operations of the Corporation. If the Corporation determines that disconnection of a Clearing Member is necessary, the Clearing Member must continue to meet its obligations to the Corporation, notwithstanding disconnection from the Corporation's systems.

(e) *Procedures for Connecting Following a Security Incident that Results in Disconnection*. In the event OCC disconnects a Clearing Member that has reported a Security Incident, upon the request of the Corporation, the Clearing Member must complete and submit a form as provided by the Corporation that describes the Security Incident and includes required representations ("Reconnection Attestation"). The Clearing Member also will be required to complete an associated checklist as provided by the Corporation that describes remediation efforts ("Reconnection Checklist").

(1) *Representations in the Reconnection Attestation.* The Reconnection Attestation must be signed by a designated senior executive of the Clearing Member who is authorized to attest to the representations required therein, including, but not limited to, the following:

(A) The Clearing Member has provided full, complete and accurate information in response to all requests made by the Corporation regarding the Security Incident, including all requests contained in the Reconnection Checklist, on a good faith, best efforts basis.

(B) The Clearing Member has provided full, complete and accurate information regarding any data or systems of the Corporation that were potentially compromised during the Security Incident, including any potential exposure of credentials used to access the Corporation's systems. The Clearing Member will immediately notify the Corporation if it later becomes aware of a previously undetected or unreported compromise of data or systems of the Corporation during the Security Incident.

(C) The Clearing Member has determined whether the Security Incident resulted, directly or indirectly, from any controls that failed or were circumvented by its employees, contractors or agents ("Failed Controls"). In a manner approved by the Corporation, the Clearing Member has communicated Failed Controls to the Corporation and is remediating or has remediated all Failed Controls.

(D) The Clearing Member has implemented, or will implement promptly, technical and operational changes, both preventative and detective, with the intent to prevent a recurrence of the Security Incident. The Clearing Member has provided written summaries of such technical and operational changes to the Corporation.

(E) The Clearing Member has complied and will continue to comply with all applicable laws in connection with its response to the Security Incident, including any notifications required to be provided to government agencies, the Corporation, and third parties.

(2) *Information Requirements in the Reconnection Checklist.* The Reconnection Checklist may require information including, but not limited to, the following: whether the disconnection was the result of a cybersecurity-related incident; the nature of the incident; the steps taken to contain the incident; the data of the Corporation, if any, that was compromised during the incident; the systems of the Corporation, if any, that were impacted during the incident; whether there was any risk of exposure of credentials used to access the systems of the Corporation, and if so, whether the credentials were reissued; the controls that were circumvented or failed that led to the incident occurring; the changes, preventative and detective, that were implemented to prevent a reoccurrence; details on how data integrity has been preserved and what data checks have been performed; whether third-parties, including government agencies, have been notified; and any additional details relevant to reconnection.