



Date: January 25, 2024

Subject: Clearing Members Cybersecurity Obligations

On November 17, 2023, the Securities and Exchange Commission issued an order approving the rule change to amend OCC Rule 219 (renumbered to OCC Rule 213) to enhance Clearing Members' cybersecurity obligations. Rule 213(d) requires Clearing Members to immediately notify OCC, in writing, if a Clearing Member becomes aware or should be aware of a security incident (as defined by the Rule). Rule 213(e) applies in the event of a disconnection of a Clearing Member from OCC system(s).

Clearing Member security incident notifications required under Rule 213(d) should be directed to CyberNotification@theocc.com. Security notifications should be made if a 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 OCC'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 OCC's data or system integrity, unauthorized disclosure of sensitive information related to OCC, or the inability of OCC to conduct essential clearance and settlement functions. Upon receipt of such notice, or if OCC has a reasonable basis to believe that a security incident has occurred, or is occurring, OCC may take any and all actions reasonably necessary to mitigate any effects to OCC's operations, including the right to disconnect access or to modify the scope and specifications of access of the Clearing Member to OCC's information and data systems.

Rule 213(e) requires that the Clearing Member provide a reconnection attestation and complete an associated reconnection checklist prior to OCC re-establishing connectivity. Clearing Members must make the following representations in the reconnection attestation:

- The Clearing Member has provided full, complete and accurate information in response to all requests from OCC;
- The Clearing Member has provided full, complete and accurate information regarding any data or systems that were potentially compromised, including any exposed credentials used to access OCC's systems;
- The Clearing member has determined whether the security incident resulted, directly or indirectly, from any controls that failed or were circumvented;
- The Clearing member has implemented or will implement technical and operation changes with the intent to prevent a reoccurrence; and
- The Clearing Member has complied and will continue to comply with all application laws in connection with its response to the security incident.

In the event this form is required, OCC will provide the form and further instructions.

Please refer to the [approved rule filing](#) for a detailed description of the changes.

If you have any questions, please contact your Clearing Member representative or the Member Services Help Desk at the following numbers: 800-621-6072 or 800-544-6091. Within Canada, please call 800-424-7320. Clearing Members may also e-mail us at memberservices@theooc.com.