THE FOUNDATION FOR SECURE MARKETS

Options Clearing Corporation
125. S. Franklin Street, Suite 1200
Chicago, IL 60606
312 322 6200 | theocc.com

June 22, 2023

VIA CFTC PORTAL
Christopher J. Kirkpatrick
Office of the Secretariat
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, N.W.
Washington, DC 20581

Re: Rule Certification by The Options Clearing Corporation Concerning Clearing Member Cybersecurity Obligations

Dear Secretary Kirkpatrick:

Pursuant to Section 5c(c)(1) of the Commodity Exchange Act, as amended ("Act"), and Commodity Futures Trading Commission ("CFTC") Regulation 40.6, The Options Clearing Corporation ("OCC") hereby certifies a rule change concerning Clearing Member Cybersecurity Obligations. The date of implementation of the rule is at least 10 business days following receipt of the certification by the CFTC. The proposal has also been submitted to the Securities and Exchange Commission ("SEC") under Section 19(b) of the Securities Exchange Act of 1934 ("Exchange Act") and Rule 19b-4 thereunder. The change will not be implemented until OCC has obtained all necessary regulatory approvals.

In conformity with the requirements of Regulation 40.6(a)(7), OCC states the following:

Explanation and Analysis

OCC proposes to amend certain provisions in OCC's Rules relating to Clearing Member cybersecurity obligations to address the occurrence of a cyber-related disruption or intrusion of a Clearing Member ("Security Incident"). The proposed changes to OCC's Rules are included as Exhibit A. Material proposed to be added to the Rules as currently in effect is underlined and material proposed to be deleted is marked in strikethrough text. All capitalized terms not defined herein have the same meaning as set forth in the OCC By-Laws and Rules.[1]

[1] OCC's By-Laws and Rules can be found on OCC's public website: https://www.theocc.com/Company-Information/Documents-and-Archives/By-Laws-and-Rules.

Overview

The proposed rule change would amend certain provisions in the Rules relating to Clearing Member cybersecurity obligations to address the occurrence of a Security Incident. The proposed changes would (i) require a Clearing Member to immediately notify OCC of a Security Incident; (ii) memorialize OCC's ability to take actions reasonably necessary to mitigate any effects to its operations; and (iii) require such Clearing Member to provide a Reconnection Attestation containing written representations addressing the incident and attesting to certain security requirements and an associated Reconnection Checklist describing remediation efforts. As described in more detail below, the proposed rule change is designed to help OCC assess and take appropriate action to manage the cybersecurity risks that may be introduced to OCC's information and data systems due to a Security Incident.

OCC believes it is prudent to implement a standardized approach to assess and manage the cybersecurity risks that OCC may face through its interconnections to Clearing Members. Cybersecurity incidents pose an ongoing risk to OCC, as well as market participants, as an attack on OCC can lead to the loss of data or system integrity, unauthorized disclosure of sensitive information, or an inability to conduct essential clearance and settlement functions. Moreover, as a designated systemically important financial market utility ("SIFMU"),[2] a failure or disruption to OCC could 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. Given its designation as a SIFMU, OCC believes it is prudent to enhance its management of Security Incidents so that OCC's own information and data systems remain protected against cyberattacks.

The proposed rule change would amend certain provisions in the Rules relating to Clearing Member cybersecurity obligations to address the occurrence of a Security Incident. Clearing Member cybersecurity obligations are currently set out in Rule 219, which addresses requirements related to a firm's cybersecurity program. The proposed rule change would expand the scope of this Rule to incorporate provisions that address the occurrence of a Security Incident, as further described below. The current Clearing Member cybersecurity obligations in this Rule would remain unchanged.

The proposed changes would clearly describe Clearing Member obligations and OCC rights with respect to a Security Incident. The proposal would require Clearing Members to immediately notify OCC of a Security Incident. OCC's notification and reporting requirements for Clearing Members are currently set forth in various provisions of the By-Laws and the Rules and require, among other things, that Clearing Members provide OCC with such documents and information as OCC may require from time to time.[3] These existing notification and reporting requirements do not directly address Security Incidents. The proposal would amend OCC's notification and reporting

---

[2] OCC was designated as a SIFMU under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010. 12 U.S.C. 5465(e)(1).

[3] See OCC Rules 302, 306A, 306B, and 308.

requirements to adopt a specific requirement in the Rules that Clearing Members immediately notify OCC of a Security Incident and promptly confirm such notice in writing.

The proposed changes would also memorialize in the Rules OCC's ability to take actions reasonably necessary to mitigate any effects of a Security Incident to its operations. OCC's existing right to disconnect access, or to modify the scope and specifications of access, of a Clearing Member to OCC information and data systems is based in the Agreement for OCC Services, which sets forth the terms of various services that OCC may provide to Clearing Members.[4] OCC maintains various contracts and forms, including the Agreement for OCC Services, that in conjunction with OCC's By-Laws and Rules, establish and govern the relationship between OCC and each Clearing Member.[5] Pursuant to the Agreement for OCC Services, OCC may terminate electronic access to particular OCC information and data systems, or modify the scope and specifications of such access, from time to time. Codifying this ability of OCC to take actions reasonably necessary to mitigate any effects to its operations in the Rules would centralize relevant information pertaining to cybersecurity in the Rules.

The proposal would further implement a standardized approach to evaluate and manage the cybersecurity risks that OCC may face due to a Security Incident. The proposal would set out new procedures that would require a Clearing Member to submit, upon OCC's request, the Reconnection Attestation and Checklist after reporting a Security Incident, both as provided by OCC from time to time. The Rule is designed to provide OCC with a degree of flexibility in requesting the Reconnection Attestation and Checklist to consider circumstances where there may be no risk or threat to OCC, such as when a Security Incident is contained to a part of a Clearing Member's business with no relevance to OCC or its markets. The Reconnection Attestation and Checklist are designed to enable OCC to determine whether the risk or threat to OCC has been mitigated sufficiently, including whether to resume connectivity to a Clearing Member if connectivity was disconnected or modified. OCC would detail specific representations and information required of Clearing Members in the proposed Reconnection Attestation and Checklist. OCC believes an attestation-based format coupled with a checklist would be most effective in ascertaining a Clearing Member's response to a Security Incident, including whether the Clearing Member has appropriate security requirements and carried out suitable remediation measures, to determine any potential threats to OCC's information and data systems. The forms filter the requested information and representations into a standardized format, which would better enable OCC to review and identify areas of interest, concern, or heightened risk in respect of a Security Incident. Standardizing the form and contents of submissions would also improve efficiency for Clearing Members and OCC by reducing the potential uncertainty and time required to demonstrate an acceptable response to a Security Incident, which would facilitate OCC's ability to evaluate the potential risk or threat posed by the Security Incident and facilitate the resumption of Clearing Member connectivity.

---

4 See Exchange Act Release No. 34-73577 (Nov. 12, 2014), 79 FR 68733 (Nov. 18, 2014) (File No. SR-OCC-2014-20).

5 Id.

Proposed Changes

The proposed rule change would amend certain provisions in the Rules relating to Clearing Member cybersecurity obligations to address the occurrence of a Security Incident. In addition to expanding the scope of existing Rules, the proposed changes would (i) require a Clearing Member to immediately notify OCC of a Security Incident; (ii) memorialize OCC's ability to take actions reasonably necessary to mitigate any effects to its operations; and (iii) require such Clearing Member to provide a Reconnection Attestation and Checklist.

Amended Cybersecurity Obligations Provisions

The proposed changes would expand the scope of existing Rule 219 to address the occurrence of a Security Incident. Existing Rule 219, titled "Cybersecurity Confirmation," currently includes requirements related to a firm's cybersecurity program and requires Clearing Members and applicants for clearing membership to submit a form, referred to as the "Cybersecurity Confirmation," that confirms the existence of a cybersecurity program. To broaden the scope, OCC proposes to retitle this Rule from "Cybersecurity Confirmation" to "Cybersecurity Obligations" to address Security Incidents and centralize cybersecurity-related provisions in one section of the Rules. For clarity, OCC also proposes to add a heading to each paragraph in this Rule to summarize its content. OCC proposes to add the following headings: "Cybersecurity Confirmation Submission" to paragraph (a), which relates to the submission of the Cybersecurity Confirmation; "Representations in the Cybersecurity Confirmation" to paragraph (b), which relates to the representations in the Cybersecurity Confirmation; and "Execution of the Cybersecurity Confirmation" to paragraph (c), which relates to the execution of the Cybersecurity Confirmation. OCC also proposes a minor edit to replace "OCC" with "the Corporation" in paragraphs (a) and (b) for consistency. Additionally, under the proposed rule change, existing Rule 219 would be renumbered as Rule 213.[6]

Occurrence of a Security Incident

The proposed changes would address the occurrence of a Security Incident in the Rules by: (i) requiring a Clearing Member to immediately notify OCC of a Security Incident; (ii) memorializing OCC's ability to take actions reasonably necessary to mitigate any effects to its operations; and (iii) requiring such Clearing Member to provide a Reconnection Attestation and Checklist. Each of these proposed changes is described in greater detail below.

---

[6] OCC proposes to renumber existing Rule 219 to Rule 213 following on proposed changes to OCC's clearing membership standards, which includes removal of current rules 213 through 218. See Exchange Act Release No. 34-97150 (Mar. 15, 2023), 88 FR 17046 (Mar. 21, 2023) (File No. SR-OCC-2023-002).

(i) Notification of a Security Incident

The proposed rule change would adopt a new paragraph (d) to amended Rule 213, titled "Occurrence of a Security Incident," to address the occurrence of a Security Incident. Proposed Rule 213(d) would define Security Incident as 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. Proposed Rule 213(d) would require a Clearing Member to immediately notify OCC if the Clearing Member becomes aware or should be aware that there has been a Security Incident or if a Security Incident is occurring and to promptly confirm such notice in writing. As a systemically important financial market utility, and the sole clearing agency providing clearing services for listed options in the U.S., it is vital that OCC's clearing systems remain functional and unaffected by Security Incidents. Any risk or threat to OCC's system(s) or operations could have a severe impact on the listed options markets. Therefore, time is of the essence with respect to any notification by a Clearing Member of the occurrence of a Security Incident. OCC intends to provide a dedicated OCC email address directly to Clearing Members for use in notifying OCC of a Security Incident, but without specifying the form of the notice. Accordingly, a Clearing Member can share information they believe is relevant, and OCC can follow up directly with the affected Clearing Member as needed.

(ii) Memorialization of OCC's Ability to Take Action

Proposed paragraph (d) to amended Rule 213 would also memorialize OCC's ability to take actions reasonably necessary to mitigate any effects to its operations in the case of a Security Incident. The proposed language specifies that upon notice from a Clearing Member of a Security Incident, or if OCC has a reasonable basis to believe that a Security Incident has occurred, or is occurring, OCC may take actions reasonably necessary to mitigate any effects to its operations. Such actions would include 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, consistent with the Agreement for OCC Services. Because of the innumerable circumstances that could lead to a Security Incident, OCC's determination to disconnect a Clearing Member will be based on the facts and circumstances related to any specific Security Incident. Accordingly, as described in proposed paragraph (d) to amended Rule 213, OCC may consider any one or more of the following in determining whether or not to disconnect a member: the potential loss of control by a Clearing Member of its internal system(s), the potential loss of OCC's confidential data, the potential strain on or loss of OCC's resources due to OCC's inability to perform clearance and settlement functions, and the overall severity of the threat to OCC's security and operations. It is OCC's belief that not all Security Incident notifications will result in a Clearing Member disconnection. However, in the event of a disconnection, a Clearing Member will remain responsible for its obligations to OCC, e.g., a Clearing Member remains responsible for the payment of margin to OCC.

(iii) Requirement to Provide Reconnection Attestation and Checklist

The proposed rule change would adopt new paragraph (e) to amended Rule 213, titled "Procedures for Connecting Following a Security Incident that Results in Disconnection," to incorporate procedures for Clearing Members to follow in the case of a Security Incident, including in order to resume connectivity to OCC. Proposed Rule 213(e) would require that 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 the Reconnection Attestation and Checklist, both as provided by OCC. The Reconnection Attestation describes the Security Incident and includes required representations, and the Checklist describes remediation efforts. Both documents facilitate OCC's ability to determine whether the risk or threat to OCC has been mitigated sufficiently, including whether to resume connectivity to a Clearing Member if connectivity was disconnected or modified. The proposed Reconnection Attestation and Checklist are set out in more detail below.

Each Reconnection Attestation would be required to be in writing on a form provided by OCC and signed by a designated senior executive of the Clearing Member who is authorized to attest to these matters, as specified in proposed Rule 213(e)(1). Each Reconnection Attestation would contain representations addressing the incident and attesting to certain security requirements. In addition, Clearing Members would be required to describe the Security Incident. OCC is proposing to require that the following representations be included in the Reconnection Attestation in proposed Rule 213(e)(1)(A) through (E):

First, the Reconnection Attestation would include a representation that the Clearing Member has provided full, complete and accurate information in response to all requests made by OCC regarding the Security Incident, including all requests contained in the Reconnection Checklist, on a good faith, best efforts basis.

Second, the Reconnection Attestation would include a representation that the Clearing Member has provided full, complete and accurate information regarding any OCC data or systems that were potentially compromised during the Security Incident, including any potential exposure of credentials used to access OCC's systems, and will immediately notify OCC if it later becomes aware of a previously undetected or unreported compromise of OCC data or systems during the Security Incident.

Third, the Reconnection Attestation would include a representation that 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"). The proposed language would further specify that the Clearing Member has communicated Failed Controls to OCC and is remediating or has remediated all Failed Controls.

Fourth, the Reconnection Attestation would include a representation that 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 and has provided written summaries of such changes to OCC.

Fifth, the Reconnection Attestation would include a representation that 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, OCC, and third parties.

Furthermore, each Reconnection Checklist would be required to be in writing on a form provided by OCC. A Clearing Member would describe its remediation efforts as part of the Reconnection Checklist, including relevant information related to the Security Incident and the Clearing Member's response thereto. To account for the evolving nature of Security Incidents, OCC proposes flexibility regarding the information requirements under proposed Rule 213(e)(2). Namely, the Reconnection Checklist may require information including, but not limited to, the following under this Rule:

- whether the disconnection was the result of a cybersecurity-related incident;
- the nature of the incident;
- the steps taken to contain the incident;
- the OCC data, if any, that was compromised during the incident;
- the OCC systems, if any, that were impacted during the incident;
- whether there was any risk of exposure of credentials used to access OCC systems, 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;[7]
- whether third-parties, including government agencies, have been notified; and
- any additional details relevant to reconnection.

Together, the required representations and information in the Reconnection Attestation and Checklist are designed to provide OCC with evidence related to a Clearing Member's response to a Security Incident, including whether the Clearing Member has appropriate security requirements and carried out suitable remediation measures, to enable OCC to better understand and manage Security Incidents. By requiring such representations and information from a Clearing Member, the Reconnection Attestation and Checklist would provide OCC with key information to make decisions about risks and threats, perform additional monitoring, and determine whether to resume connectivity to a Clearing Member, as applicable, in order to protect OCC's information and data systems.

---

[7] OCC notes that the Reconnection Checklist would specifically request details on how data integrity has been preserved and what data checks have been performed "prior to reconnecting to and sending/receiving data to/from OCC."

Consistency with DCO Core Principles

OCC reviewed the DCO core principles ("Core Principles") as set forth in the Act, the regulations thereunder, and the provisions applicable to a DCO that elects to be subject to the provisions of 17 CFR Subpart C ("Subpart C DCO"). During this review, OCC identified the following as potentially being impacted:

Risk management. OCC believes that the proposed changes are consistent with Core Principle D.[8] CFTC Regulation 39.13[9] requires, in relevant part, that each DCO ensure that it possesses the ability to manage the risks associated with discharging the responsibilities of the DCO through the use of appropriate tools and procedures.[10] As described above, the proposed amendments are designed to help OCC assess and take appropriate action to manage the cybersecurity risks that may be introduced to OCC's information and data systems due to a Security Incident.

OCC proposes edits to existing Rule 219, including to titles and headings, to expand the scope to address the occurrence of a Security Incident. Existing Rule 219 would be renumbered as Rule 213 and would clearly set out the obligation of Clearing Members to notify OCC of a Security Incident and the right of OCC to take actions reasonably necessary to mitigate any effects to its operations, thereby centralizing relevant information pertaining to cybersecurity in the Rules and promoting transparency. Moreover, the proposal would implement a standardized approach to assess and manage the cybersecurity risks that OCC may face through its interconnections to Clearing Members. The proposal would include procedures for Clearing Members to follow in the case of a Security Incident, including in order to resume connectivity to OCC. The proposed changes would require a Clearing Member to submit, upon OCC's request, the Reconnection Attestation and Checklist after reporting a Security Incident, both as provided by OCC. OCC proposes to set forth specific representations and information required of Clearing Members in the Reconnection Attestation and Checklist, which are designed to provide OCC with evidence related to a Clearing Member's response to a Security Incident, including whether the Clearing Member has appropriate security requirements and carried out suitable remediation measures, to enable OCC to better understand and manage Security Incidents. The Reconnection Attestation and Checklist would provide OCC with key information to make decisions about risks and threats, perform additional monitoring, and determine whether to resume connectivity to a Clearing Member, as applicable, to protect OCC's information and data systems. In this way, OCC believes the proposed change is consistent with Core Principle D under the Act. [11]

---

8 7 U.S.C. 7a-1(c)(2)(D).

9 17 CFR 39.13.

10 17 CFR 39.13(a).

11 7 U.S.C. 7a-1(c)(2)(D).

Systems safeguards. OCC believes that the proposed changes are consistent with the requirements of Core Principle I.[12] CFTC Regulation 39.18[13] requires, in relevant part, that each DCO establish and maintain a program of risk analysis and oversight with respect to its operations and automated systems to identify and minimize sources of operational risk through (i) the development of appropriate controls and procedures; and (ii) the development of automated systems that are reliable, secure and have adequate scalable capacity.[14]

With respect to (i), the proposed Reconnection Attestation and Checklist would reduce the cybersecurity risks to OCC by requiring a Clearing Member to provide written representations addressing the incident and attesting to certain security requirements and an associated checklist describing remediation efforts. The proposed Reconnection Attestation and Checklist would filter the requested information and representations into a standardized format, which would better enable OCC to review and identify areas of interest, concern, or heightened risk in respect of a Security Incident. The representations and information in these forms would help OCC mitigate its exposure to cybersecurity risk and, thereby, decrease the operational risks to OCC. The proposed Reconnection Attestation and Checklist would identify to OCC potential sources of external operational risks that may be introduced through its interconnections to Clearing Members and enable OCC to mitigate these risks and possible impacts to OCC's operations. Based on this information, OCC would make a determination regarding the resumption of connectivity to a Clearing Member if connectivity was disconnected or modified. As a result, OCC believes the proposal is consistent with the requirements of Core Principle I under the Act. [15]

With respect to (ii), the proposed Reconnection Attestation and Checklist would help enhance the security, resiliency, and operational reliability of OCC's information and data systems. Namely, these forms would help OCC determine whether to take action against a Clearing Member, including preventing the reconnection of a Clearing Member, that may pose an increased cyber risk to OCC by not having appropriate security requirements or taking suitable remediation measures. Clearing Members that have not adequately addressed Security Incidents may present increased risk to OCC. For example, weaknesses within a Clearing Member's environment could allow for exploitation by a malicious actor of the link between a Clearing Member and OCC. By better enabling OCC to identify these risks, the proposed rule change would allow OCC to more effectively secure its environment against potential vulnerabilities. The required representations and information in the Reconnection Attestation and Checklist would provide OCC with key information to make decisions about risks and threats, perform additional monitoring, and determine whether to resume connectivity to a Clearing Member, as applicable, to protect OCC's information and data systems. As a result, OCC believes the proposal would improve OCC's ability to ensure that its

---

12 7 U.S.C. 7a-1(c)(2)(I).

13 17 CFR 39.18(b).

14 17 CFR 39.18(b)(1).

15 7 U.S.C. 7a-1(c)(2)(I).

systems have a high degree of security, resiliency, and operational reliability, and, as such, is consistent with the requirements of Core Principle I under the Act.[16]

Treatment of funds. OCC believes the proposed changes are consistent with Core Principle F,[17] and CFTC Regulation 39.15 which requires, in part, that each DCO establish standards and procedures that are designed to protect and ensure the safety of funds and assets belonging to clearing members and their customers.[18] Risks, threats, and potential vulnerabilities could impact OCC's ability to clear and settle securities transactions, or to safeguard the securities and funds which are in its custody or control, or for which it is responsible. Therefore, by enhancing its processes to mitigate these risks through implementation of standardized procedures for Clearing Members to follow in the case of a Security Incident, OCC believes the proposal 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 the clearing agency or for which it is responsible, consistent with the Core Principle F under the Act.[19]

For these reasons, OCC believes that the proposed changes are consistent with the requirements of the DCO Core Principles and the CFTC Regulations thereunder.

Opposing Views

On April 25, 2023 and April 26, 2023, the SEC received comments on proposed rule change SR-OCC-2023-003 (the "Initial Filing") filed by OCC. The comments addressed the scope of the proposed definition of "Security Incident" and potential conflicts with other existing and proposed SEC rules. OCC filed Partial Amendment No.1 to the Initial Filing to clarify what constitutes a Security Incident, the standards for determining whether to disconnect a Clearing Member, and the process for reconnection. OCC has incorporated changes from Partial Amendment No. 1 into this rule certification.

Notice of Pending Rule Certification

OCC hereby certifies that notice of this rule filing has been given to Clearing Members of OCC in compliance with Regulation 40.6(a)(2) by posting a copy of this certification on OCC's website concurrently with the filing of this submission.

---

16 Id.

17 7 U.S.C. 7a-1(c)(2)(F)(i).

18 17 CFR 39.15(a).

19 7 U.S.C. 7a-1(c)(2)(F).

Certification

OCC hereby certifies that the rule set forth at Exhibit A of the enclosed filing complies with the Act and the CFTC's regulations thereunder.

Should you have any questions regarding this matter, please do not hesitate to contact me.

Sincerely,

/s/ **Megan Cahill**
Megan Cahill
Assistant General Counsel
The Options Clearing Corporation

Enclosure: Exhibit A