SECURITIES AND EXCHANGE COMMISSION
(Release No. 34-98979; File No. SR-OCC-2023-003)

November 17, 2023

Self-Regulatory Organizations; The Options Clearing Corporation; Order Granting Approval of Proposed Rule Change, as Modified by Partial Amendment No. 1, Concerning Clearing Member Cybersecurity Obligations

I. INTRODUCTION

On March 21, 2023, the Options Clearing Corporation ("OCC") filed with the Securities and Exchange Commission ("Commission") the proposed rule change SR-OCC-2023-003 pursuant to Section 19(b) of the Securities Exchange Act of 1934 ("Exchange Act")[1] and Rule 19b-4[2] thereunder. The proposed rule change would amend certain provisions in OCC's Rules relating to each Clearing Member's obligation to address a "Security Incident" (*i.e.*, the occurrence of a cyber-related disruption or intrusion of a Clearing Member's systems that is reasonably likely to pose an imminent risk or threat to OCC's operations) of that Clearing Member. The proposed rule change was published for public comment in the *Federal Register* on April 5, 2023.[3] The Commission has received comments regarding the proposed rule change.[4]

On May 18, 2023, pursuant to the Section 19(b)(2) of the Exchange Act,[5] the Commission designated a longer period within which to approve, disapprove, or institute

---

1 15 U.S.C. 78s(b)(1).

2 17 CFR 240.19b-4.

3 Securities Exchange Act Release No. 97225 (Mar. 30, 2023), 88 FR 20195 (Apr. 5, 2023) (File No. SR-OCC-2023-003) ("Notice of Filing").

4 Comments on the proposed rule change are available at *https://www.sec.gov/comments/sr-occ-2023-003/srocc2023003.htm*.

5 15 U.S.C. 78s(b)(2).

proceedings to determine whether to approve the proposed rule change.[6] On May 24, 2023, OCC filed Partial Amendment No. 1 to the Notice of Filing.[7] For the reasons discussed below, the Commission is approving the proposed rule change, as modified by Partial Amendment No. 1 (hereinafter, "proposed rule change").

II. BACKGROUND

Currently, the only OCC Rule governing a Clearing Member's cybersecurity obligations to OCC is Rule 219, titled "Cybersecurity Confirmation."[8] It requires Clearing Members and applicants for clearing membership to submit to OCC a form called the "Cybersecurity Confirmation" at least every two years or as part of its application materials. Through the form, Clearing Members and applicants confirm that they maintain a comprehensive cybersecurity program that meets certain criteria (*e.g.*, the cybersecurity program is approved by senior management, it is reviewed and updated periodically, the cybersecurity program is designed to protect the segment of the Clearing Member's or applicant's system that interacts with OCC, it includes a process for the Clearing Member to remediate cyber issues, etc.). However, current Rule 219 does not require Clearing Members to notify OCC if they experience a cybersecurity incident that could impact OCC or otherwise address OCC's processes, or the Clearing Member's obligations with respect to OCC.

---

6 *See* Securities Exchange Act Release No. 97525 (May 18, 2023), 88 FR 33655 (May 24, 2023) (File No. SR-OCC-2023-003).

7 *See* Securities Exchange Act Release No. 97602 (May 26, 2023), 88 FR 36351 (June 2, 2023) (File No. SR-OCC-2023-003) ("Notice of Partial Amendment"). OCC submitted Partial Amendment No. 1 in response to comments regarding the proposed definition of "Security Incident" for purposes of proposed Rule 213(d), the notification requirements and procedure in the event of a Security Incident, factors considered when determining whether to disconnect or reduce a clearing member's access, and clarification related to reconnection.

8 Capitalized terms used but not defined herein have the meanings specified in OCC's Rules and By-Laws, available at *https://www.theocc.com/about/publications/bylaws.jsp*.

The proposed rule change would renumber Rule 219 as Rule 213 and rename the rule "Cybersecurity Obligations" to reflect the expanded scope of the Rule.[9] It also would add section headings to the Rule and replace references to "OCC" with references to "the Corporation," but otherwise would not change the provisions regarding the existing Cybersecurity Confirmation form that confirms the existence of a Clearing Member's cybersecurity program.[10]

The substantive changes to the Rule would be the addition of two new subsections—(d) and (e)—titled "Occurrence of a Security Incident" and "Procedures for Connecting Following a Security Incident," respectively. New subsection (d) would require a Clearing Member to immediately notify OCC if the member becomes aware or should be aware of a Security Incident (as defined in the Rule). It would also specify that OCC may take actions reasonably necessary to mitigate any effects on its operations following a Security Incident. New subsection (e) would require a Clearing Member wishing to reconnect its systems to OCC's systems to provide OCC with a new form, titled "Reconnection Attestation," that describes the Security Incident and attests to certain security requirements, as well as an associated checklist, titled "Reconnection Checklist," that describes the affected Clearing Member's remediation efforts and other key information. Each of these proposed changes is described in greater detail below.

---

9 The renumbering follows proposed changes to OCC's clearing membership standards, which includes removal of current Rules 213 through 218. *See* Securities Exchange Act Release No. 97150 (Mar. 15, 2023), 88 FR 17046 (Mar. 21, 2023) (File No. SR-OCC-2023-002).

10 Specifically, OCC would add the following headings: "Cybersecurity Confirmation Submission" to paragraph (a); "Representations in the Cybersecurity Confirmation" to paragraph (b); and "Execution of the Cybersecurity Confirmation" to paragraph (c).

A. New Paragraph (d): Occurrence of a Security Incident

Proposed Rule 213(d) would define a Security Incident as an incident that has occurred or 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.[11] To provide guidance regarding the types of disruptions or intrusions that might be considered Security Incidents, the proposed rule includes a non-exhaustive list of examples. Specifically, a Security Incident may include any disruption or degradation of the normal operation of the Clearing Member's systems or any unauthorized entry into the Clearing Member's systems that would result in loss of OCC's data or system integrity, an unauthorized disclosure of sensitive information related to OCC, or the inability of OCC to conduct essential clearance and settlement functions.[12]

Under the proposed rule, a Clearing Member would be required to immediately notify OCC if the member becomes aware or should be aware that there has been a Security Incident or that a Security Incident is occurring.[13] The Clearing Member would also need to promptly confirm such notice in writing.

The proposed rule would specify that, if OCC receives notice of a Security Incident from a Clearing Member or has a reasonable basis to believe a Security Incident has occurred or is occurring, OCC may take actions reasonably necessary to mitigate any effects to its operations,

---

11 In response to public comment, OCC amended the proposed rule change to specify that a disruption or intrusion of a Clearing Member's systems would only be deemed a Security Incident if it is "reasonably likely to pose an imminent risk or threat to OCC's operations." *See* Notice of Partial Amendment, 88 FR at 36352.

12 In response to public comment, OCC added the non-exhaustive list of potential Security Incidents to clarify that the focus of the Rule would be on the potential impact on OCC of a disruption or intrusion. *See* Notice of Partial Amendment, 88 FR at 36352.

13 *See* Notice of Partial Amendment, 88 FR at 36352.

including disconnecting the Clearing Member's access to OCC's information and data systems or modifying the scope and specifications of such access. Finally, paragraph (d) of the proposed rule would provide a non-exhaustive list of factors OCC may consider in determining whether to modify a Clearing Member's access to OCC's information and data systems, up to and including disconnection, in response to a Security Incident. Specifically, among other factors, OCC may consider 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 the security and operations of OCC.[14] Further, if the Corporation reasonably 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.

B. New Paragraph (e): Procedures for Connecting Following a Security Incident that Results in Disconnection

Proposed Rule 213(e) would clarify the process for a Clearing Member to request reconnection to OCC's systems following disconnection as a result of a Security Incident. In particular, the Clearing Member would need to complete and submit, upon OCC's request, a new form referred to by OCC as the "Reconnection Attestation" and a related checklist referred to by OCC as the "Reconnection Checklist." The Reconnection Attestation would include a text box for the Clearing Member to provide a narrative description of the Security Incident and five representations to which, by signing the form, the Clearing Member would be attesting.

---

[14] In response to public comment, OCC amended its proposed rule to specify that these are the types of factors OCC would consider when determining whether to disconnect a Clearing Member. *See* Notice of Partial Amendment, 88 FR at 36353. OCC also clarified its anticipation that not all Security Incident notifications will result in a Clearing Member disconnection. *See id.* at 36352.

Specifically, by signing the Reconnection Attestation, the Clearing Member would be attesting that it 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;
- 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;
- 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");[15]
- 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; and
- 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.[16]

---

[15] The proposed language would further specify that the Clearing Member has communicated the existence of Failed Controls to OCC and is remediating or has remediated all Failed Controls.

[16] *See* proposed Rule 213(e)(1)(A) through (E). Further, each Reconnection Attestation must be provided in writing and signed by a designated senior executive of the Clearing Member.

The associated Reconnection Checklist would include questions designed to elicit additional details regarding the Security Incident, including the potential cause of the incident, steps taken to contain it, the exposure and impact to OCC's systems or data, the Clearing Member's remediation efforts, and any other details relevant to the Clearing Member's request to reconnect to OCC's systems. The Reconnection Checklist would require the Clearing Member to respond to the following questions:[17]

- was the disconnection the result of a cybersecurity-related incident;
- describe the nature of the incident;
- what steps were taken to contain the incident;
- what OCC data, if any, was compromised during the incident;
- what OCC systems, if any, were impacted during the incident;
- was there any risk of exposure of credentials used to access OCC systems and, if so, were the credentials reissued;
- which controls were circumvented or failed that led to the incident occurring;
- what changes, preventative and detective, were implemented to prevent a reoccurrence;
- how has data integrity been preserved and what data checks have been performed prior to reconnecting to and sending/receiving data to/from OCC;
- have third-parties, including government agencies, been notified; and
- any additional details relevant to reconnection.[18]

---

17 The description of the checklist provided here is based on the Exhibit 3 to File No. SR-OCC-2023-003 provided by OCC at the time of filing.

18 These are the specific questions included in the Reconnection Checklist that OCC submitted as Exhibit 3 to the proposed rule change. *See* Exhibit 3 to File No. SR OCC2023-003. However, proposed Rule 213(e)(2) specifies that the Reconnection Checklist may require "information including, but not limited to," the 11 questions noted above. This is to account for the evolving nature of Security Incidents and provide OCC

According to OCC, the Reconnection Attestation and Reconnection Checklist are designed to accomplish several goals. First, they are designed to enable OCC to determine whether the risk or threat to OCC has been mitigated sufficiently for OCC to resume connectivity to the Clearing Member.[19] Second, they 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 more broadly.[20] Finally, they would better enable OCC to identify areas of interest, concern, or heightened risk by presenting information in a standardized format.[21]

III. DISCUSSION AND COMMISSION FINDINGS

Section 19(b)(2)(C) of the Exchange Act directs the Commission to approve a proposed rule change of a self-regulatory organization if it finds that such proposed rule change is consistent with the requirements of the Exchange Act and the rules and regulations thereunder applicable to such organization.[22] Under the Commission's Rules of Practice, the "burden to demonstrate that a proposed rule change is consistent with the Exchange Act and the rules and regulations issued thereunder . . . is on the self-regulatory organization ['SRO'] that proposed the rule change."[23]

The description of a proposed rule change, its purpose and operation, its effect, and a

---

with flexibility to modify the specific information requirements if necessary. *See* Notice of Filing, 88 FR at 20196.

19 *See* Notice of Filing, 88 FR at 20196.

20 *Id.* at 20197.

21 *Id.*

22 15 U.S.C. 78s(b)(2)(C).

23 Rule 700(b)(3), Commission Rules of Practice, 17 CFR 201.700(b)(3).

legal analysis of its consistency with applicable requirements must all be sufficiently detailed and specific to support an affirmative Commission finding,[24] and any failure of an SRO to provide this information may result in the Commission not having a sufficient basis to make an affirmative finding that a proposed rule change is consistent with the Exchange Act and the applicable rules and regulations.[25] Moreover, "unquestioning reliance" on an SRO's representations in a proposed rule change is not sufficient to justify Commission approval of a proposed rule change.[26]

After carefully considering the proposed rule change, the Commission finds that the proposed rule change is consistent with the requirements of the Exchange Act and the rules and regulations thereunder applicable to OCC. More specifically, the Commission finds that the proposal is consistent with Section 17A(b)(3)(F) of the Exchange Act[27] and Rule 17Ad-22(e)(17)(i)[28] thereunder as described in detail below.

A. *Consistency with Section 17A(b)(3)(F) of the Exchange Act*

Section 17A(b)(3)(F) of the Exchange Act requires, among other things, that a clearing agency's rules are designed to promote the prompt and accurate clearance and settlement of securities transactions.[29] In addition to centralizing relevant information pertaining to Clearing Member Security Incidents in a single rule, the proposed rule change is designed to support OCC's management of potential cybersecurity risks by enhancing OCC's ability to identify and

---

24 *Id.*

25 *Id.*

26 Susquehanna Int'l Group, LLP v. Securities and Exchange Commission, 866 F.3d 442, 447 (D.C. Cir. 2017) ("Susquehanna").

27 15 U.S.C. 78q-1(b)(3)(F).

28 17 CFR 240.17Ad-22(e)(17)(i).

29 15 U.S.C. 78q-1(b)(3)(F).

mitigate cybersecurity risks posed by a Security Incident experienced by one of OCC's Clearing Members. It also is designed to standardize OCC's cybersecurity risk management practices with respect to such Security Incidents. Among other things, the changes set forth Clearing Member obligations and the actions OCC may take if reasonably necessary to mitigate the effects of a Security Incident on its operations. As discussed further below, the changes also strengthen OCC's ability to manage its cyber-related risks by requiring Clearing Members to immediately notify OCC if the Clearing Member becomes aware of or should be aware that there has been a Security Incident or one is occurring, and promptly confirm such a notice in writing. Taken together, the proposed changes should strengthen OCC's cybersecurity risk management processes. By creating a consistent set of obligations on Clearing Members for identifying and reporting Security Incidents, OCC would enhance its ability to monitor, mitigate, and manage cybersecurity risks—such as unauthorized disclosure of sensitive information or a loss of data or system integrity—in the event a Clearing Member experiences a Security Incident. Because OCC's information, data, and systems support and enable OCC's ability to conduct essential clearance and settlement functions, enhancing OCC's ability to limit the impact of a Security Incident at a Clearing Member promotes OCC's ability to continue the prompt and accurate clearance and settlement of securities transactions.

Accordingly, and for the reasons discussed below, the proposal is consistent with the requirements of Section 17A(b)(3)(F) of the Exchange Act.

B. *Consistency with Rule 17Ad-22(e)(17)(i) of the Exchange Act*

Rule 17Ad-22(e)(17)(i) requires that a covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to manage the covered clearing agency's operational risks by identifying the plausible sources of operational risk, both

internal and external, and mitigating their impact through the use of appropriate systems, policies, procedures, and controls.[30] In adopting Rule 17Ad-22(e)(17)(i), the Commission provided guidance, stating that a covered clearing agency generally should consider, among other things, whether it identifies, monitors, and manages the risks that key participants pose to its operations.[31] To the extent they interact with OCC's systems, Clearing Member systems may present operational risk to OCC. As described above, OCC proposes requiring members to report any cyber-related disruption or intrusion that could pose a risk to OCC's operations, such as a degradation of normal operations that would result in the inability of OCC to conduct essential clearance and settlement functions. OCC also proposes numerous protective measures, such as the ability to take reasonably necessary actions to mitigate the effects of a Security Incident on its operations, including disconnecting the Clearing Member's access to OCC's systems; the ability to consider a non-exhaustive list of factors to determine whether to modify a Clearing Member's access to OCC's systems in response to a Security Incident, up to and including disconnection; and the requirement for disconnected Clearing Members to complete a Reconnection Attestation and Reconnection Checklist that OCC would review and evaluate as part of a determination to reconnect the Clearing Member to OCC's systems. Taken together, these proposals support OCC's ability to effectively identify, monitor, and manage the risks that Clearing Members pose to OCC operations, and are therefore consistent with Rule 17Ad-22(e)(17)(i).

---

30 17 CFR 240.17Ad-22(e)(17)(i).

31 *See* Standards for Covered Clearing Agencies, Securities Exchange Act Release No. 78961 (Sept. 28, 2016), 81 FR 70786, 70838 (Oct. 13, 2016).

A commenter opposed the proposal on a number of grounds.[32] Specifically, the commenter expressed concerns about the proposed definition of Security Incident, stating that because the proposed definition applies to all of a Clearing Member's systems and therefore could include an incident that would not affect OCC systems, the definition is inconsistent with the risks identified by OCC in the rule filing, other regulatory and SRO requirements, and is potentially beyond the scope of OCC's authority.[33] The commenter also stated that OCC's proposed definition of Security Incident is inconsistent with other regulatory and SRO requirements because it does not require that a loss or harm has occurred and it does not require that a clearing member be aware of the incident.[34] The commenter stated that the definition of Security Incident should be limited to an incident that could result in "loss of data or system integrity," "unauthorized disclosure of sensitive information," or "an inability [for the OCC] to conduct essential clearance and settlement functions."[35] The commenter further requested clarification that the reference to "disruption or degradation of a clearing member's systems" in the proposed definition of Security Incident is limited to cyber-related disruptions or intrusions resulting from malicious third-party activity as opposed to, for example, a power outage.[36]

OCC responded by amending the proposed rule change in a number of ways.[37] First, OCC amended the definition of Security Incident to limit it to a cyber-related disruption or

---

32 *See* letter from Howard Meyerson, Managing Director, Financial Information Forum ("FIF"), dated April 26, 2023, to Vanessa Countryman, Secretary, Commission ("FIF Letter").

33 *Id.* at 2 – 3. FIF stated that, as drafted, a Security Incident could include an incident that would not affect OCC systems and this approach appears to be overly broad with the risks identified in the proposed rule change, indicating that the reference to "disruption or degradation of a clearing member's systems" in the proposed definition of Security Incident is ambiguous. *Id.* at 2.

34 *Id.* at 4 – 5.

35 *Id.* at 3.

36 *Id.* at 5 – 6.

37 *See* Notice of Partial Amendment *supra* note 7.

intrusion of the Clearing Member's systems that is reasonably likely to pose an imminent risk or threat to OCC's operations.[38] OCC further amended the definition of Security Incident to state that such an incident may include, but is not limited to, any disruption or degradation of the normal operation of the Clearing Member's systems or any unauthorized entry into the Clearing Member's systems 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.[39] In amending the Security Incident definition this way, OCC reasonably addressed the commenter's concerns about the scope of the rule by clarifying that only occurrences that present certain risks or threats to OCC's operations are considered Security Incidents, and provided examples to help illustrate the types of risks and threats to OCC's operation that are covered by the rule. In response to the commenter's concern that the proposed definition of Security Incident does not require that a clearing member be aware of the Incident, OCC also amended the proposed definition to require notice only if the Clearing Member becomes aware or should be aware that such an incident has occurred or is occurring.[40] The commenter further stated that OCC "should incorporate into the notice provision a [condition] that only requires reporting when a clearing member has a reasonable basis to conclude that a reportable cybersecurity incident has occurred or determines that a reportable cybersecurity incident has occurred."[41] As noted, OCC amended the proposed definition to require reporting only where a Clearing Member becomes or should be aware of a Security Incident. The proposed rule change therefore would require Clearing Members to engage in

---

38 *Id.*

39 *Id.*

40 *Id.*

41 FIF Letter at 5.

reasonable diligence to obtain and report to OCC readily discoverable information about a Security Incident, consistent with the Clearing Member's current obligation to maintain a comprehensive cybersecurity program that, among other things, is designed to protect the segment of the Clearing Member's system that interacts with OCC, but it would not require reporting of a cybersecurity incident if the member could not reasonably be aware of such an incident. OCC's response reasonably balances the commenter's concern about being required to report unknown information and OCC's need to ensure that its Clearing Members are diligently monitoring their own systems so that OCC can identify, monitor, and manage the impact of a Security Incident at a Clearing Member on OCC's systems and operations, as well as the listed options markets generally.

A commenter stated that the content of the notification should be limited in scope given the requirement for "immediate" notification, and recommended that OCC should provide more detail about the expected content in the notification.[42] The commenter also expressed the view that the need for immediate written notice "does not provide a clearing member with the opportunity to evaluate the incident prior to reporting."[43] OCC addressed these comments in the amendment by clarifying the notification requirements and procedure in the event of a Security Incident. Specifically, because there are "innumerable circumstances that could lead to a Security Incident," rather than requiring the notice to include specific, pre-determined content, OCC clarified that a Clearing Member can share information it believes is relevant, and that OCC can follow up directly as needed.[44] OCC also noted that, given the urgency required to

---

42 *Id*. at 5-6.

43 *Id*. at 5.

44 *See* Notice of Partial Amendment, 88 FR at 36352.

address a Security Incident quickly and remain functional as a systemically important financial market utility, OCC will provide a dedicated email address for Clearing Members to provide OCC with written notification (or confirmation) of a Security Incident.[45] By clarifying that the notice is limited to information the affected Clearing Member believes is relevant and that OCC can follow up directly with the Clearing Member as needed, OCC's response reasonably balances the commenter's concern about the rule not specifying what information needs to be included in the notice and OCC's need to identify, monitor, and manage the impact of a Security Incident at a Clearing Member on OCC's systems and operations, as well as the listed options markets generally. Allowing Clearing Members to provide the information they believe is relevant together with OCC's ability to gather additional information as necessary and appropriate helps ensure that OCC gets timely information on Security Incidents, which supports OCC's ability to identify, monitor, and manage risks posed to its operations,[46] consistent with the Commission's guidance regarding Rule 17Ad-22(e)(17)(i).

A commenter stated that OCC should enumerate threshold conditions that must be satisfied before OCC could disconnect or modify a Clearing Member's access.[47] The commenter further requested clarification on the relationship between the proposed Security Incident notifications and the proposed disconnection and reconnection process.[48] In response, as noted above, OCC amended the definition of Security Incident to limit it to a cyber-related disruption

---

45 *See id*.

46 The clarification provided by OCC also addresses a commenter concern that the disclosure should "take into account the fact that target firms often have incomplete information about a cybersecurity incident and engage in an investigative process over a period of time." FIF Letter at 7. OCC's ability to follow up directly as needed ensures that Clearing Members will have an opportunity to provide additional information as facts develop.

47 *Id.* at 6 – 7.

48 *Id.* at 7.

or intrusion of the Clearing Member's systems that is reasonably likely to pose an imminent risk or threat to OCC's operations.[49] OCC also stated that because there are "innumerable circumstances that could lead to a Security Incident," such a determination would require an evaluation of the specific facts and circumstances related to the Security Incident, and amended the proposed rule to include a non-exhaustive list of factors OCC will consider when making a disconnection determination.[50] Specifically, as amended, the rule provides that 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. By amending the definition of a Security Incident in this way, OCC identified the threshold condition that must be satisfied before OCC could disconnect or modify a Clearing Member's access in response to a Security Incident. Specifically, unless the Clearing Member experiences a cyber-related disruption or intrusion of the Clearing Member's system that is reasonably likely to pose an imminent risk or threat to OCC's operations, OCC would not have a basis under the proposed rule to disconnect or modify a Clearing Member's access to OCC systems. Further, disconnection or modification of a Clearing Member's access to OCC's systems is not an automatic consequence in the event a Clearing Member notifies OCC of a Security Incident. OCC stated that it believes that not all Security Incident notifications will result in a Clearing Member disconnection, and the proposed rule does not mandate disconnection in response to a Security Incident. Rather, disconnection or

---

49 *See* Notice of Partial Amendment *supra* note 7.

50 *See* Notice of Partial Amendment, 88 FR at 36353.

modification of access are among the various mitigation actions that OCC may take if it determines that it is reasonably necessary to do so to mitigate a Security Incident's effects on its operations. In addition, OCC's non-exhaustive list of factors provides examples of specific risks or threats to OCC's operations that OCC would consider as factors in making a disconnection determination, and that are consistent with the Commission's guidance related to Rule 17Ad-22(e)(17)(i). Given the extensive variety and rapidly evolving nature of cyber-related threats, it is reasonable for OCC to balance its need to evaluate the specific facts and circumstances of each cyber-related incident at a Clearing Member and the desire of Clearing Members to know in advance the specific conditions that could result in a disconnection or modification of its access to OCC's systems. OCC's proposed approach of defining a single, specific threshold condition—namely, a cyber-related disruption or intrusion of the Clearing Member's system reasonably likely to pose an imminent risk or threat to OCC's operations—while providing an illustrative list of factors OCC will consider as it makes a disconnection determination, strikes this balance.

By making these amendments, OCC also clarified the connection between a Security Incident notification and the proposed disconnection and reconnection process. If OCC determines that disconnection is reasonably necessary to mitigate any effects to its operations, the process for the affected Clearing Member to reconnect to OCC's systems following the disconnection are set forth in paragraph (e) of proposed rule 213, "Procedures for Connecting Following a Security Incident." Additionally, OCC amended the proposed rule to require a Clearing Member to complete the Reconnection Attestation and Reconnection Checklist only in the event that OCC disconnected the Clearing Member that has reported a Security Incident.[51]

---

[51] *Id.*

The information provided in the Reconnection Attestation and Reconnection Checklist would help OCC determine whether the risk to OCC has been mitigated sufficiently for OCC to resume connectivity to the Clearing Member. Taken together, these changes as well would allow OCC to identify and mitigate operational risks presented by its Clearing Members and secure its environment more effectively against potential vulnerabilities.

A commenter stated that the Reconnection Checklist appears to be a security incident notification form rather than a checklist for reconnection.[52] As discussed above, the Reconnection Checklist is only required in the event that a Clearing Member is disconnected from OCC's systems as the result of a Security Incident. The checklist includes information such as the nature of the incident, the steps taken to contain the incident, and any OCC data that was compromised during the incident, all of which is used by OCC to determine whether the risk to OCC posed by the Security Incident has been mitigated sufficiently to resume the Clearing Member's connectivity. The commenter also stated that the proposed rule should establish a clear process for reconnection, including the process and timing for OCC to decide on a reconnection request and the process for OCC to communicate its determination.[53] As noted above, the process for reconnection is set forth in paragraph (e) of proposed Rule 213. In addition, although the proposed rule does not mandate the specific timing for OCC to make a reconnection determination, the information provided to OCC by the Reconnection Attestation and Reconnection Checklist is designed to facilitate OCC's reconnection determinations, which should help expedite the process. Given the innumerable circumstances that could lead to a Security Incident and a resulting disconnection, the proposed rule strikes a reasonable balance

52 FIF Letter at 8.

53 *Id.*

between OCC's need to ensure that the operational risks presented by a Security Incident at a Clearing Member have been sufficiently mitigated before reconnecting to OCC's systems and the Clearing Member's desire to reconnect as quickly as possible.

A commenter expressed concern that the information required to be disclosed in Reconnection Checklist and Attestation is too detailed and could either provide a roadmap to malicious actors or subject the Clearing Member to third-party litigation risk.[54] The commenter also requested clarification on the protection of information reported by Clearing Members to OCC.[55] Any information disclosed to OCC in a Reconnection Checklist and Attestation would be kept confidential by OCC and would not be made publicly available, including to third parties and potential malicious actors, and therefore would not, by virtue of being provided to OCC, provide a roadmap to malicious actors or subject the reporting Clearing Member to third-party litigation risk. Further, OCC routinely receives, and is responsible for the protection of, confidential information related to its Clearing Members. For example, OCC routinely receives and protects confidential and sensitive information related Clearing Members' risk management practices,[56] as well as information related to any financial or operational difficulty reported by Clearing Members to any regulatory organization.[57]

The commenter also stated that OCC should provide an exception to disclosure when law enforcement directs the member not to disclose.[58] However, the lack of the type of law

---

54 *Id*. at 7 – 8. For example, the commenter expressed concern that the level of detail required by the proposed rule change could provide a roadmap for malicious actors who wish to gain access to OCC's systems or could present third-party litigation risk to the Clearing Member.

55 *Id*. at 6.

56 *See* OCC Rule 305(b).

57 *See* OCC Rule 306A(1).

58 FIF Letter at 6.

enforcement exception suggested by the commenter is consistent with the Exchange Act. For example, OCC's current rules, as approved by the Commission, include various reporting and disclosure requirements, none of which provide the type of explicit law enforcement exception suggested by the commenter.[59]

The commenter also questioned whether the Clearing Members should be required to provide evidence of regulatory compliance to other government agencies and third parties.[60] OCC's current rules, as approved by the Commission, require Clearing Members to notify OCC if the Clearing Member is required to notify any regulatory organization of any operational difficulty affecting the Clearing Member, or of any failure by the Clearing Member to be in compliance with the operational responsibility rules of any regulatory organization.[61] Thus, a Clearing Member that experiences a Security Incident that subjects the Clearing Member to a regulatory notification requirement is already required, under existing OCC Rules, to notify OCC that it complied with that requirement. The proposed rule change does not create a new obligation for Clearing Members to notify OCC of regulatory notices to regulatory organizations; it merely specifies when a notification to OCC in connection with a Security Incident must be provided.

---

59 *See, e.g.*, OCC Rules 207 (Submission to and Retrieval of Items to and from the Corporation) and 306A (Event-Based Reporting).

60 FIF Letter at 7. The commenter stated that many clearing members would be subject to numerous governmental and third-party notification requirements in the event of a cybersecurity incident and expressed confusion regarding why OCC would require an attestation relating to a clearing member's notification to other regulators and third-parties if the clearing member has provided all required notifications to the OCC. *Id.* The commenter also stated that any required attestation should be to the knowledge of the attesting executive. The proposed rule change states explicitly that the representations in the Reconnection Attestation would be made "on a good faith, best efforts basis," which necessarily means the attestation would be to the knowledge of the attesting executive. *See* proposed Rule 213(e)(1)(A).

61 *See* OCC Rule 306A (Event-Based Reporting).

Finally, a commenter referenced a number of cybersecurity-related rule proposals recently published by the Commission and stated that the proposed rule change should be delayed at least until the Commission finalizes all the currently proposed cybersecurity rulemaking to ensure that investors are protected from cyber threats and unnecessary additional burdens are not placed on OCC Clearing Members.[62] The commenter states further that the proposed rule change interconnects and may overlap with four different rules proposed by the Commission,[63] and requests that the Commission extend the period for comment on the proposed rule change to allow time to analyze the proposed rule change alongside the rules proposed by the Commission.[64]

Under the Exchange Act and relevant rules thereunder, SROs, including OCC, determine for themselves when to file a proposed rule change. The Exchange Act defines the process and time within which the Commission may act,[65] and Section 19(b)(2)(C) of the Exchange Act requires the Commission to approve a proposed rule change of a SRO if it finds that such change is consistent with the Exchange Act and rules and regulations thereunder that are applicable to the SRO.[66] Concerns regarding rules proposed by the Commission may be presented as

---

62 *See* letter from Melissa MacGregor, Managing Director, Deputy General Counsel & Corporate Secretary, SIFMA, dated April 25, 2023, to Vanessa Countryman, Secretary, Commission, ("SIFMA Letter") available at *https://www.sec.gov/comments/sr-occ-2023-003/srocc2023003-20164982-334488.pdf*. A similar perspective was provided by a second commenter. *See* FIF Letter at 8 – 9; *see also* Securities Exchange Act Release Nos. 97141 (Mar. 15, 2022), 88 FR 20616 (Apr. 6, 2023); 97142 (Mar. 15, 2022), 88 FR 20212 (Apr. 5, 2023); 97143 (Mar. 15, 2023), 88 FR 23146 (Apr. 14, 2023); 97144 (Mar. 15, 2023), 88 FR 16921 (Mar. 21, 2023); 94382 (Mar. 9, 2022), 87 FR 16590 (Mar. 23, 2022).

63 SIFMA Letter at 2. SIFMA does not state how the proposed rule change interconnects or conflicts with the Commission's proposed rules.

64 *Id.* This concern was echoed in a letter from the FIF. *See* FIF Letter (stating that OCC should withdraw the proposed rule change and resubmit after the comment periods for the Commission's proposals have expired).

65 *See, e.g.*, 15 U.S.C. 78s(b)(2)(A)(ii) (allowing the Commission to extend the period for review by not more than 45 days if the Commission determines that a longer period is appropriate and publishes the reasons for such determination).

66 15 U.S.C. 78s(b)(2)(C).

comments to such rules so that the Commission may consider them in determining what, if any, final rule it will adopt.

Based on the foregoing, the Commission finds that the proposed rule change is consistent with the requirements of Rule 17Ad-22(e)(17)(i) under the Exchange Act.[67]

[67] 17 CFR 240.17Ad-22(e)(17)(i).

IV. CONCLUSION

On the basis of the foregoing, the Commission finds that the proposed rule change, as modified by Partial Amendment No. 1, is consistent with the requirements of the Exchange Act, and in particular, the requirements of Section 17A of the Exchange Act[68] and the rules and regulations thereunder.

IT IS THEREFORE ORDERED, pursuant to Section 19(b)(2) of the Exchange Act,[69] that the proposed rule change (SR-OCC-2023-003), as modified by Partial Amendment No. 1, be, and hereby is, approved.

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.[70]

Sherry R. Haywood,

Assistant Secretary.

---

68 In approving this proposed rule change, the Commission has considered the proposed rules' impact on efficiency, competition, and capital formation. *See* 15 U.S.C. 78c(f).

69 15 U.S.C. 78s(b)(2).

70 17 CFR 200.30-3(a)(12).