Required fields are shown with yellow backgrounds and asterisks.

Page 1 of * 45

SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549
Form 19b-4

File No. * SR 2023 - * 003
Amendment No. (req. for Amendments *)

Filing by Options Clearing Corporation

Pursuant to Rule 19b-4 under the Securities Exchange Act of 1934

Initial * ☑ Amendment * ☐ Withdrawal ☐

Section 19(b)(2) * ☑ Section 19(b)(3)(A) * ☐ Section 19(b)(3)(B) * ☐

Pilot ☐

Extension of Time Period for Commission Action * ☐

Date Expires *

Rule

☐ 19b-4(f)(1) ☐ 19b-4(f)(4)
☐ 19b-4(f)(2) ☐ 19b-4(f)(5)
☐ 19b-4(f)(3) ☐ 19b-4(f)(6)

Notice of proposed change pursuant to the Payment, Clearing, and Settlement Act of 2010

Section 806(e)(1) * ☐ Section 806(e)(2) * ☐

Security-Based Swap Submission pursuant to the Securities Exchange Act of 1934
Section 3C(b)(2) * ☐

Exhibit 2 Sent As Paper Document ☐

Exhibit 3 Sent As Paper Document ☐

Description

Provide a brief description of the action (limit 250 characters, required when Initial is checked *).

Proposed rule change by The Options Clearing Corporation concerning Clearing Member cybersecurity obligations.

Contact Information

Provide the name, telephone number, and e-mail address of the person on the staff of the self-regulatory organization prepared to respond to questions and comments on the action.

First Name * [redacted] Last Name * [redacted]

Title * [redacted]

E-mail * rulefilings@theocc.com

Telephone * (312) 322-6200 Fax

Signature

Pursuant to the requirements of the Securities Exchange of 1934, Options Clearing Corporation has duty caused this filing to be signed on its behalf by the undersigned thereunto duty authorized.

Date 03/21/2023

By [redacted]
(Name *)

(Title *) [redacted]

NOTE: Clicking the signature block at right will initiate digitally signing the form. A digital signature is as legally binding as a physical signature, and once signed, this form cannot be changed.

[redacted]

Required fields are shown with yellow backgrounds and astericks.

SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

For complete Form 19b-4 instructions please refer to the EFFS website.

Form 19b-4 Information *

Add | Remove | View

SR-OCC-2023-003 (Cyber) 19b-4 (03

The self-regulatory organization must provide all required information, presented in a clear and comprehensible manner, to enable the public to provide meaningful comment on the proposal and for the Commission to determine whether the proposal is consistent with the Act and applicable rules and regulations under the Act.

Exhibit 1 - Notice of Proposed Rule Change *

Add | Remove | View

SR-OCC-2023-003 (Cyber) Exhibit 1A

The Notice section of this Form 19b-4 must comply with the guidelines for publication in the Federal Register as well as any requirements for electronic filing as published by the Commission (if applicable). The Office of the Federal Register (OFR) offers guidance on Federal Register publication requirements in the Federal Register Document Drafting Handbook, October 1998 Revision. For example, all references to the federal securities laws must include the corresponding cite to the United States Code in a footnote. All references to SEC rules must include the corresponding cite to the Code of Federal Regulations in a footnote. All references to Securities Exchange Act Releases must include the release number, release date, Federal Register cite, Federal Register date, and corresponding file number (e.g., SR-[SRO]-xx-xx). A material failure to comply with these guidelines will result in the proposed rule change being deemed not properly filed. See also Rule 0-3 under the Act (17 CFR 240.0-3)

Exhibit 1A - Notice of Proposed Rule Change, Security-Based Swap Submission, or Advanced Notice by Clearing Agencies *

Add | Remove | View

The Notice section of this Form 19b-4 must comply with the guidelines for publication in the Federal Register as well as any requirements for electronic filing as published by the Commission (if applicable). The Office of the Federal Register (OFR) offers guidance on Federal Register publication requirements in the Federal Register Document Drafting Handbook, October 1998 Revision. For example, all references to the federal securities laws must include the corresponding cite to the United States Code in a footnote. All references to SEC rules must include the corresponding cite to the Code of Federal Regulations in a footnote. All references to Securities Exchange Act Releases must include the release number, release date, Federal Register cite, Federal Register date, and corresponding file number (e.g., SR-[SRO]-xx-xx). A material failure to comply with these guidelines will result in the proposed rule change being deemed not properly filed. See also Rule 0-3 under the Act (17 CFR 240.0-3)

Exhibit 2- Notices, Written Comments, Transcripts, Other Communications

Add | Remove | View

Copies of notices, written comments, transcripts, other communications. If such documents cannot be filed electronically in accordance with Instruction F, they shall be filed in accordance with Instruction G.

☐ Exhibit Sent As Paper Document

Exhibit 3 - Form, Report, or Questionnaire

Add | Remove | View

SR-OCC-2023-003 (Cyber) Exhibit 3 (

Copies of any form, report, or questionnaire that the self-regulatory organization proposes to use to help implement or operate the proposed rule change, or that is referred to by the proposed rule change.

☐ Exhibit Sent As Paper Document

Exhibit 4 - Marked Copies

Add | Remove | View

The full text shall be marked, in any convenient manner, to indicate additions to and deletions from the immediately preceding filing. The purpose of Exhibit 4 is to permit the staff to identify immediately the changes made from the text of the rule with which it has been working.

Exhibit 5 - Proposed Rule Text

Add | Remove | View

SR-OCC-2023-003 (Cyber) Exhibit 5 (

The self-regulatory organization may choose to attach as Exhibit 5 proposed changes to rule text in place of providing it in Item I and which may otherwise be more easily readable if provided separately from Form 19b-4. Exhibit 5 shall be considered part of the proposed rule change

Partial Amendment

Add | Remove | View

If the self-regulatory organization is amending only part of the text of a lengthy proposed rule change, it may, with the Commission's permission, file only those portions of the text of the proposed rule change in which changes are being made if the filing (i.e. partial amendment) is clearly understandable on its face. Such partial amendment shall be clearly identified and marked to show deletions and additions.

SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

Form 19b-4

Proposed Rule Change
by

THE OPTIONS CLEARING CORPORATION

Pursuant to Rule 19b-4 under the
Securities Exchange Act of 1934

Item 1. Text of the Proposed Rule Change

Pursuant to the provisions of Section 19(b)(1) of the Securities Exchange Act of 1934 ("Exchange Act" or "Act"),[1] and Rule 19b-4 thereunder,[2] The Options Clearing Corporation ("OCC" or "Corporation") is filing with the Securities and Exchange Commission ("Commission") a proposed rule change 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 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 form containing written representations addressing the incident and attesting to certain security requirements ("Reconnection Attestation") and an associated checklist describing remediation efforts ("Reconnection Checklist" and together, "Reconnection Attestation and Checklist").

The proposed changes to OCC's Rules are included as Exhibit 5 to File No. SR-OCC-2023-003. 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.[3]

Item 2. Procedures of the Self-Regulatory Organization

The proposed changes were approved for filing with the Commission by the Board of Directors of OCC at a meeting held on December 15, 2022.

---

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

2 17 CFR 240.19b-4.

3 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.

Item 3. Self-Regulatory Organization's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

A. Purpose

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"),[4] 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

[4] 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).

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.[5] These existing notification and reporting requirements do not directly address Security Incidents. The proposal would amend OCC's notification and reporting 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

---

5 See Article V, Section 1, Interpretation and Policy .07 of the By-Laws and Rules 201(b), 215, 216, 217(b), 303, 306, 308 and 310(a)-(c).

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.[6] 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.[7] 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

---

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

7 Id.

representations and information required of Clearing Members in the proposed Reconnection Attestation and Checklist, included in Exhibit 3 to File No. SR-OCC-2023-003. 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.

Proposed Rule 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.[8]

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.

---

[8] 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, including, but 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. Proposed Rule 213(d) would require a Clearing Member to immediately notify OCC if there has been a Security Incident or if a Security Incident is occurring and to promptly confirm such notice in writing.

(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.

(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," 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 a Clearing Member to complete and

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 Reconnection Attestation and Checklist would 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;[9]
- 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.

---

9 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." See Exhibit 3 to File No. SR-OCC-2023-003.

B. Statutory Basis

OCC believes the proposed rule changes are consistent with the requirements of the Act and the rules and regulations thereunder applicable to a registered clearing agency. In particular, OCC believes that the proposed rule changes are consistent with Section 17A(b)(3)(F) of the Act,[10] and Rules 17Ad-22(e)(17)(i) and (e)(17)(ii), each promulgated under the Act,[11] for the reasons described below.

Section 17A(b)(3)(F) of the Act requires that the rules of OCC be designed to, among other things, 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.[12] 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

---

10 15 U.S.C. 78q-1(b)(3)(F).

11 17 CFR 240.17Ad-22(e)(17)(i) and (e)(17)(ii).

12 15 U.S.C. 78q-1(b)(3)(F).

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 from time to time. 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. 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, 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 requirements of Section 17A(b)(3)(F) of the Act.[13]

Rule 17Ad-22(e)(17)(i) under the Act requires that each 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

---

13 Id.

appropriate systems, policies, procedures, and controls.[14] 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 Rule 17Ad-22(e)(17)(i) under the Act.[15]

Rule 17Ad-22(e)(17)(ii) under the Act requires that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to manage the covered clearing agency's operational risks by ensuring, in part, that systems have a high degree of security, resiliency, and operational reliability.[16] 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

---

14 17 CFR 240.17Ad-22(e)(17)(i).

15 Id.

16 17 CFR 240.17Ad-22(e)(17)(ii).

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 systems have a high degree of security, resiliency, and operational reliability, and, as such, is consistent with the requirements of Rule 17Ad-22(e)(17)(ii) under the Act.[17]

Item 4. Self-Regulatory Organization's Statement on Burden on Competition

Section 17A(b)(3)(I) of the Act[18] requires that the rules of a clearing agency not impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act. OCC does not believe that the proposed rule changes would impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act. As discussed above, OCC proposes to 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)

---

17 Id.

18 15 U.S.C. 78q-1(b)(3)(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. While the proposed changes would require Clearing Members to incur additional costs, including to complete and submit the Reconnection Attestation and Checklist, OCC does not believe the proposed changes would present an undue burden on Clearing Members. Clearing Members are already subject to the notification and reporting requirements in OCC's By-Laws and the Rules that require, among other things, that Clearing Members provide OCC with such documents and information as OCC may require from time to time.[19] Standardizing the form and contents of the proposed submissions would reduce the potential uncertainty and time required to demonstrate an acceptable response to a Security Incident. Additionally, the proposed changes would not unfairly inhibit access to OCC's services or disadvantage or favor any particular user in relationship to another user. Such changes would apply to all Clearing Members consistently and thus would not provide any Clearing Member with a competitive advantage over any other Clearing Member as the requirements would be uniform. As described above, given OCC's position in the marketplace, OCC believes it is prudent to enhance its management of Security Incidents as detailed in the proposal, so that OCC's own information and data systems remain protected against cyberattacks. For the foregoing reasons, OCC believes that the proposed rule change is in the public interest, would be consistent with the requirements of the Act applicable to clearing agencies, and would not impact or impose a burden on competition.

---

[19] See Article V, Section 1, Interpretation and Policy .07 of the By-Laws and Rules 201(b), 215, 216, 217(b), 303, 306, 308 and 310(a)-(c).

Item 5. Self-Regulatory Organization's Statement on Comments on the Proposed Rule Change Received from Members, Participants, or Others

Written comments were not and are not intended to be solicited with respect to the proposed rule change, and none have been received.

Item 6. Extension of Time Period for Commission Action

Not applicable.

Item 7. Basis for Summary Effectiveness Pursuant to Section 19(b)(3) or for Accelerated Effectiveness Pursuant to Section 19(b)(2) or Section 19(b)(7)(D)

Not applicable.

Item 8. Proposed Rule Change Based on Rules of Another Self-Regulatory Organization or of the Commission

Not applicable.

Item 9. Security-Based Swap Submissions Filed Pursuant to Section 3C of the Act

Not applicable.

Item 10. Advance Notices Filed Pursuant to Section 806(e) of the Payment, Clearing and Settlement Supervision Act

Not applicable.

Item 11. Exhibits

Exhibit 1A. Completed Notice of Proposed Rule Change for publication in the Federal Register.

Exhibit 3. OCC Reconnection Attestation and Reconnection Checklist forms.

Exhibit 5. Proposed changes to the Rules.

EXHIBIT 1A

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

[March __, 2023]

Self-Regulatory Organizations; The Options Clearing Corporation; Notice of Filing of Proposed Rule Change by The Options Clearing Corporation Concerning Clearing Member Cybersecurity Obligations

Pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 ("Exchange Act" or "Act"),[1] and Rule 19b-4 thereunder,[2] notice is hereby given that on March 21, 2023, The Options Clearing Corporation ("OCC" or "Corporation") filed with the Securities and Exchange Commission ("SEC" or "Commission") the proposed rule change as described in Items I, II, and III below, which Items have been prepared primarily by OCC. The Commission is publishing this notice to solicit comments on the proposed rule change from interested persons.

I. Clearing Agency's Statement of the Terms of Substance of the Proposed Rule Change

The proposed rule change would 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 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 form containing written representations addressing the incident and attesting to certain security requirements ("Reconnection Attestation") and an associated checklist

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

2 17 CFR 240.19b-4.

describing remediation efforts ("Reconnection Checklist" and together, "Reconnection Attestation and Checklist").

The proposed changes to OCC's Rules are included as Exhibit 5 to File No. SR-OCC-2023-003. 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.[3]

II. Clearing Agency's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

In its filing with the Commission, OCC included statements concerning the purpose of and basis for the proposed rule change and discussed any comments it received on the proposed rule change. The text of these statements may be examined at the places specified in Item IV below. OCC has prepared summaries, set forth in sections (A), (B), and (C) below, of the most significant aspects of these statements.

(A) Clearing Agency's Statement of the Purpose of, and Statutory Basis for, the Proposed Rule Change

(1) Purpose

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

---

[3] 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.

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"),[4] 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,

---

4 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).

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.[5] These existing notification and reporting requirements do not directly address Security Incidents. The proposal would amend OCC's notification and reporting 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.[6] OCC maintains various contracts and

---

5 See Article V, Section 1, Interpretation and Policy .07 of the By-Laws and Rules 201(b), 215, 216, 217(b), 303, 306, 308 and 310(a)-(c).

6 See Exchange Act Release No. 34-73577 (Nov. 12, 2014), 79 FR 68733 (Nov. 18,

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.[7] 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, included in Exhibit 3 to File No. SR-OCC-2023-003. OCC believes an attestation-based format coupled with a checklist would be most effective in ascertaining

---

2014) (File No. SR-OCC-2014-20).

7 Id.

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.

Proposed Rule 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.[8]

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.

---

8 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, including, but 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. Proposed Rule 213(d) would require a Clearing Member to immediately notify OCC if there has been a Security Incident or if a Security Incident is occurring and to promptly confirm such notice in writing.

(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.

(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," 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 a Clearing Member to complete and 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 Reconnection Attestation and Checklist would 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;[9]
- 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

---

[9] 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." See Exhibit 3 to File No. SR-OCC-2023-003.

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.

(2) Statutory Basis

OCC believes the proposed rule changes are consistent with the requirements of the Act and the rules and regulations thereunder applicable to a registered clearing agency. In particular, OCC believes that the proposed rule changes are consistent with Section 17A(b)(3)(F) of the Act,[10] and Rules 17Ad-22(e)(17)(i) and (e)(17)(ii), each promulgated under the Act,[11] for the reasons described below.

Section 17A(b)(3)(F) of the Act requires that the rules of OCC be designed to, among other things, 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.[12] 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

---

10 15 U.S.C. 78q-1(b)(3)(F).

11 17 CFR 240.17Ad-22(e)(17)(i) and (e)(17)(ii).

12 15 U.S.C. 78q-1(b)(3)(F).

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 from time to time. 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. 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, 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 requirements of Section 17A(b)(3)(F) of the Act.[13]

Rule 17Ad-22(e)(17)(i) under the Act requires that each 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.[14] 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

---

13 Id.

14 17 CFR 240.17Ad-22(e)(17)(i).

believes the proposal is consistent with the requirements of Rule 17Ad-22(e)(17)(i) under the Act.[15]

Rule 17Ad-22(e)(17)(ii) under the Act requires that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to manage the covered clearing agency's operational risks by ensuring, in part, that systems have a high degree of security, resiliency, and operational reliability.[16] 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 systems have a high degree of security,

---

15 Id.

16 17 CFR 240.17Ad-22(e)(17)(ii).

resiliency, and operational reliability, and, as such, is consistent with the requirements of Rule 17Ad-22(e)(17)(ii) under the Act.[17]

(B) Clearing Agency's Statement on Burden on Competition

Section 17A(b)(3)(I) of the Act[18] requires that the rules of a clearing agency not impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act. OCC does not believe that the proposed rule changes would impose any burden on competition not necessary or appropriate in furtherance of the purposes of the Act. As discussed above, OCC proposes to 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 and Checklist. While the proposed changes would require Clearing Members to incur additional costs, including to complete and submit the Reconnection Attestation and Checklist, OCC does not believe the proposed changes would present an undue burden on Clearing Members. Clearing Members are already subject to the notification and reporting requirements in OCC's By-Laws and the Rules that require, among other things, that Clearing Members provide OCC with such documents and information as OCC may require from time to time.[19] Standardizing the form and contents of the proposed submissions would reduce the

---

17 Id.

18 15 U.S.C. 78q-1(b)(3)(I).

19 See Article V, Section 1, Interpretation and Policy .07 of the By-Laws and Rules 201(b), 215, 216, 217(b), 303, 306, 308 and 310(a)-(c).

potential uncertainty and time required to demonstrate an acceptable response to a Security Incident. Additionally, the proposed changes would not unfairly inhibit access to OCC's services or disadvantage or favor any particular user in relationship to another user. Such changes would apply to all Clearing Members consistently and thus would not provide any Clearing Member with a competitive advantage over any other Clearing Member as the requirements would be uniform. As described above, given OCC's position in the marketplace, OCC believes it is prudent to enhance its management of Security Incidents as detailed in the proposal, so that OCC's own information and data systems remain protected against cyberattacks. For the foregoing reasons, OCC believes that the proposed rule change is in the public interest, would be consistent with the requirements of the Act applicable to clearing agencies, and would not impact or impose a burden on competition.

(C) Clearing Agency's Statement on Comments on the Proposed Rule Change Received from Members, Participants or Others

Written comments were not and are not intended to be solicited with respect to the proposed rule change and none have been received.

III. Date of Effectiveness of the Proposed Rule Change and Timing for Commission Action

Within 45 days of the date of publication of this notice in the Federal Register or within such longer period up to 90 days (i) as the Commission may designate if it finds such longer period to be appropriate and publishes its reasons for so finding or (ii) as to which the self-regulatory organization consents, the Commission will:

(A) by order approve or disapprove such proposed rule change, or

(B) institute proceedings to determine whether the proposed rule change should be disapproved.

The proposal shall not take effect until all regulatory actions required with respect to the proposal are completed.

IV. Solicitation of Comments

Interested persons are invited to submit written data, views and arguments concerning the foregoing, including whether the proposed rule change is consistent with the Act. Comments may be submitted by any of the following methods:

Electronic Comments:

- Use the Commission's Internet comment form (http://www.sec.gov/rules/sro.shtml); or
- Send an e-mail to rule-comments@sec.gov. Please include File Number SR-OCC-2023-003 on the subject line.

Paper Comments:

- Send paper comments in triplicate to Vanessa Countryman, Secretary, Securities and Exchange Commission, 100 F Street, NE, Washington, DC 20549-1090.

All submissions should refer to File Number SR-OCC-2023-003. This file number should be included on the subject line if e-mail is used. To help the Commission process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's Internet website (http://www.sec.gov/rules/sro.shtml). Copies of the submission, all subsequent amendments, all written statements with respect to the proposed rule change that are filed with the Commission, and all written communications relating to the proposed rule change between the Commission and any person, other than those that may be withheld from the public in accordance with the provisions of 5 U.S.C. 552, will be available for website viewing and printing in the Commission's Public Reference Room, 100 F Street,

NE, Washington, DC 20549, on official business days between the hours of 10:00 a.m. and 3:00 p.m. Copies of such filing also will be available for inspection and copying at the principal office of OCC and on OCC's website at https://www.theocc.com/Company-Information/Documents-and-Archives/By-Laws-and-Rules.

All comments received will be posted without change. Persons submitting comments are cautioned that we do not redact or edit personal identifying information from comment submissions. You should submit only information that you wish to make available publicly.

All submissions should refer to File Number SR-OCC-2023-003 and should be submitted on or before [insert date 21 days from publication in the Federal Register].

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.[20]

Secretary

---

[20] 17 CFR 200.30-3(a)(12).

EXHIBIT 3

OPTIONS CLEARING CORPORATION CONFIRMATION OF CYBERSECURITY PROGRAM IN CONNECTION WITH RECONNECTING TO OCC FOLLOWING A SECURITY INCIDENT

The Options Clearing Corporation
125 S. Franklin St.
Chicago, IL 60606

Legal Entity Name: _____**(the "Company")**

Attention: Company Control Officer Name: _____

Description of the security incident experienced by the Company (the "Security Incident")

CONFIRMATION

The Company has designated the Company Control Officer indicated below with sufficient authority to be responsible and accountable for overseeing and executing the cybersecurity program within the organization.

- The Company has provided full, complete and accurate information to OCC in response to all requests made by OCC regarding the Security Incident, including all requests contained in the OCC and Third Party Reconnection Checklist. The Company has provided this information on a good faith, best efforts basis.

- The Company has provided OCC with 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. The Company will immediately notify OCC if the Company later becomes aware of a previously undetected or unreported compromise of OCC data or systems during the Security Incident.

- The Company has determined whether the Security Incident resulted, directly or indirectly, from any controls that failed or were circumvented by the Company's employees, contractors or agents (the "**Failed Controls**"). In a manner approved by OCC, the Company has communicated Failed Controls to OCC and is remediating or has remediated all Failed Controls.

- The Company 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 Company has provided written summaries of such technical and operational changes to OCC.

- The Company 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 OCC, and third parties.

I am the designated Control Officer authorized to attest to the above on behalf of the Company.

COMPANY: _____

First Name: _____ **Last Name:** _____

Phone: _____ **Email:** _____

Title: _____ **Date:** _____

Signature: _____

THE FOUNDATION FOR SECURE MARKETS℠

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

OCC and Third Party Reconnection Checklist

This form must be completed to assist OCC in determining the status of remediation efforts. OCC will use this information, in part, to determine when services/connections may be restored.

Please have the Senior Executive in charge of Information Security or delegate provide the information requested in this letter and return to OCC in the manner agreed to at the time of the request.

Entity Name Address	
Date Completed	
Completed by Name Title Email Phone Number	
Senior Executive in charge of Information Security Name Email Phone Number	

1. Was the disconnection the result of a cybersecurity-related incident?

2. Please describe the nature of the incident.

3. What steps were taken to contain the incident?

4. To the best of your knowledge, what, if any, OCC data was compromised during the incident?

5. To the best of your knowledge, what, if any, OCC systems were impacted during the incident?

6. During the incident, was there any risk of exposure of credentials used to access OCC systems? If so, have the credentials been reissued? Please provide details on how many passwords were rotated, work in progress with OCC to rotate SSH keys and usernames, and what is left to complete.

7. Which controls were circumvented or failed that led to the incident occurring?

8. What changes, preventative and detective, have been implemented to prevent a reoccurrence, i.e., what steps were implemented to provide high confidence the cyber risk to OCC has been mitigated?

9. Please provide 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.

10. Have you notified any third-parties, including government agencies?

11. Please provide any additional details you feel are relevant to reconnection.

EXHIBIT 5

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 there has been an incident, or an incident is occurring, involving a cyber-related disruption or intrusion of the Clearing Member, including, but 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 ("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.

(e) *Procedures for Connecting Following a Security Incident.* After a Clearing Member reports a Security Incident, upon the request of the Corporation, the Clearing Member must complete and submit a form that describes the Security Incident and includes required representations as determined by the Corporation ("Reconnection Attestation") and an associated checklist that describes remediation efforts and provides required information as determined by the Corporation ("Reconnection Checklist"), both as provided by the Corporation from time to time.

(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.