

Required fields are shown with yellow backgrounds and asterisks.

Page 1 of * 108

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

File No. * SR 2026 - * 010

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 revisions to OCC Rule 213 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 *

[REDACTED]

Fax

[REDACTED]

Signature

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

Date

10/08/2026

(Title *)

By

[REDACTED]

(Name *)

[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.

Digitally signed by [REDACTED]

Date: 2026.10.08 16:08:46
-05'00'

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 EDFS website.

Form 19b-4 Information *

Add Remove View

SR-OCC-2026-010_19b-4 OCC Revis

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-2026-010_Exhibit 1A.docx

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-2026-010 Exhibit 3 Cover Pa

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-2026-010_Exhibit 5 OCC Ru

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”) is filing with the Securities and Exchange Commission (“Commission”) a proposed rule change to amend OCC Rule 213 – Cybersecurity Obligations (“Rule 213”) to further enhance OCC’s security protocols and promote resiliency in OCC’s approach to assessing and managing cybersecurity risks. OCC’s proposed changes to Rule 213 would, among other things, (i) establish the concept of a “Major Clearing Member System Event,” in which OCC would be authorized to take certain action, including disconnection of a Clearing Member, or its Third-Party Service Provider, connected to OCC’s Systems (as defined below); (ii) enhance the requirements of a Clearing Member to notify OCC in the event of a Security Incident (which would be redefined as a “Clearing Member System Event”); (iii) remove language that invites a Clearing Member to assess potential impact of a Clearing Member System Event on OCC’s Systems and clarify OCC’s authority to assess such incident and determine impact; (iv) provide OCC with the authority to inform, or require the Clearing Member to inform, the Clearing Member’s Third-Party Service Provider (as defined below) of the Clearing Member System Event; (v) update and add defined terms used throughout Rule 213; and (vi) incorporate other reporting, testing and approval requirements, process, obligations, and governance necessary for reconnection.

The proposed changes to OCC Rule 213 are contained in Exhibit 5 to File No. SR-OCC-2026-010. Material proposed to be added is marked by underlining and material proposed to be

¹ 15 U.S.C. 78s(b)(1).

² 17 CFR 240.19b-4.

deleted is marked with strikethrough text. All terms with initial capitalization that are not otherwise 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 change was approved for filing with the Commission by OCC's Board of Directors ("Board") at a meeting held on February 27, 2026, and by the Technology Committee of the Board at a meeting held on February 26, 2026.

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

A. Purpose

Background

OCC is the sole clearing agency for standardized equity options listed on national securities exchanges registered with the Commission. OCC provides clearing services for options on equities, indices, Exchange Traded Funds ("ETFs"), for certain transactions in futures and options on futures, and for certain stock loan transactions. Organizations become OCC Clearing Members to facilitate the clearing and settlement of their customer transactions or proprietary transactions through OCC. More specifically, in its role as a clearing agency, OCC guarantees the performance of its Clearing Members for all transactions cleared by OCC by becoming the buyer to every seller and the seller to every buyer (or the lender to every borrower and the borrower to every lender, in the case of stock loan transactions). In 2012, OCC was designated as a systemically important financial market utility ("SIFMU") by the Financial Stability Oversight Council pursuant to Title VIII of the Dodd-Frank Wall Street Reform and

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>.

Consumer Protection Act of 2010 (“Dodd-Frank Act”)⁴. Such designation highlights the critical role that OCC plays in ensuring the stability and integrity of the financial markets.

Based on OCC’s interconnections with its Clearing Members and with its Clearing Member’s Third-Party Service Provider connected to OCC’s Systems, OCC is exposed to various cybersecurity risks. Such cybersecurity risks have the potential to impact OCC, as well as market participants, as a cybersecurity attack on OCC may 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 SIFMU, a failure or disruption to OCC could threaten the stability of the financial system in the United States. Therefore, OCC believes it is prudent to enhance the cybersecurity notification obligations of its Clearing Members and strengthen OCC’s ability to protect against and respond to such events to safeguard OCC’s Systems and information against cyberattacks.

In November 2023, OCC received approval⁵ from the Commission to amend certain provisions in OCC’s Rules relating to a Clearing Member’s obligation to address a “Security Incident” (currently defined as 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). The amended provisions became OCC’s existing Rule 213, which established, among other things: (i) notification requirements of a Clearing Member in the event of a Security Incident and (ii) OCC’s security requirements for the reconnection process of a Clearing Member following a Security Incident that results in a Clearing Member’s disconnection.

⁴ Financial Stability Oversight Council 2012 Annual Report, Appendix A: Designation of Systemically Important Financial Market Utilities, at 145 (2012), <https://home.treasury.gov/system/files/261/2012-Appendix-A-Designation-of-Systemically-Important-Market-Utilities.pdf>.

⁵ See Securities Exchange Act Release No. 98979 (Nov. 17, 2023), 88 FR 82441 (Nov. 24, 2023) (SR–OCC–2023–003).

In recent years, OCC has received Rule 213 notifications, however, none have impacted OCC. OCC monitors the threat landscape on an ongoing basis, maintaining a dedicated threat intelligence team responsible for monitoring the activities of threat actors targeting the financial services industry. Through this monitoring, OCC has observed an increase in the frequency and elevated risk of cyber events targeting the industry and the broader marketplace. Considering OCC's experience receiving Rule 213 notifications, together with the increasing frequency and elevated risk of cyber events in the financial services industry at large, OCC has identified opportunities for additional enhancements to Rule 213. Though no specific triggering event necessitated these enhancements, OCC's actions are proactive, taken in light of the elevated risk environment across the industry.

OCC's proposed amendments to Rule 213 are intended to further promote resiliency, strengthen OCC's cybersecurity protocols, and maintain consistency with industry standards, including by aligning OCC's Rules with recent rule amendments⁶ of similarly situated self-regulatory organizations ("SROs") with overlapping membership with OCC. Among other things, OCC's proposed enhancements to Rule 213 would:

- Add a defined terms section to Rule 213, including defining OCC's "Systems" to include not only direct connections, but also established communication channels (e.g., access to File Transfer Protocols ("FTPs") for transmitting data or instructions that may be compromised by a systems intrusion to a Clearing Member's back-office systems);

⁶ See Securities Exchange Act Release No.104183 (Nov. 17, 2025), 90 FR 52453 (Nov. 20, 2025) (SR-DTC-2025-003), (SR-FICC-2025-006), (SR-NSCC-2025-003).

- Require the Cybersecurity Confirmation to be signed by a senior executive of the Clearing Member or applicant who is authorized to attest to such matters;
- Remove language that invites a Clearing Member to assess the potential impact of a Clearing Member System Event on OCC's Systems and operations when determining whether such incident is reportable, specify the timeframe in which OCC requires a Clearing Member System Event to be reported, and identify the specific information a Clearing Member must include in such notice;
- Establish the concept of a "Major Clearing Member System Event," including a declaration requiring the approval of two or more Designated Officers and prompt notification to the Chairman of the Board of Directors;
- Reorganize and clarify OCC's authority to take action in response to a Clearing Member System Event, including specifying the actions that constitute a "disconnect," and clarify a Clearing Member's related cooperation obligations;
- Add provisions incorporating the reporting, testing, and approval requirements, process, obligations, and governance necessary for reconnection, including the ability for OCC to require an audit report from a Third-Party Cybersecurity Firm; and
- Provide OCC with the authority to inform, or require the Clearing Member to inform, the Clearing Member's Third-Party Service Provider of the Clearing Member System Event if OCC determines, in its discretion, that such action is necessary for the protection of OCC and other Clearing Members.

As described in more detail below, OCC believes its proposed changes will strengthen OCC's security protocols by enhancing Rule 213 to be more efficient, effective and clear in its

cybersecurity obligations of Clearing Members so that OCC may better address cybersecurity risks to protect OCC and its Clearing Members. Furthermore, OCC believes its proposed changes will enable OCC's Clearing Members to better understand and prepare for their obligations to OCC as it relates to a cybersecurity event.

Proposed Changes

Proposed Rule 213(a)⁷ – Defined Terms

First, OCC proposes to introduce new section (a) titled "Defined Terms." To strengthen the provisions of proposed Rule 213 and further clarify OCC's requirements related to the cybersecurity obligations of a Clearing Member, OCC proposes to define several terms specifically for the purposes of Rule 213.⁸ OCC's proposed changes would:

- Define "Best Practices" to mean policies, procedures, practices or similar standards and guidelines that are reasonably designed and consistent with then current financial-sector cybersecurity standards issued by an authoritative body that is a U.S. governmental entity or agency, an association of a U.S. governmental entity or agency, or a widely recognized industry organization. The purpose of defining "Best Practices" is to clarify the standards that OCC would require a Third-Party Cybersecurity Firm to employ when such firm is engaged, as would be required by OCC Rule 213 as discussed further below. OCC's proposed definition of "Best Practices" aligns with Section 1001(a)(4) of the Commission's Regulation Systems Compliance and Integrity ("Reg SCI").⁹

⁷ Existing Rule 213(a) would be renumbered to Rule 213(b).

⁸ OCC's proposed amendments to Rule 213 align with the rule amendments of similarly situated SROs with overlapping membership with OCC, including the National Securities Clearing Corporation ("NSCC"). See supra note 6.

⁹ 17 CFR 242.1001(a)(4).

- Delete OCC’s existing definition of a “Security Incident” and replace it with “Clearing Member System Event.” OCC proposes to define a “Clearing Member System Event” to mean an incident resulting from the unintended or unauthorized access to, or the malfunction or corruption (whether partial or total) of one or more systems, of a Clearing Member or its Third-Party Service Provider, connected to OCC’s Systems. The purpose of re-defining the concept of a “Security Incident” to a “Clearing Member System Event” is to capture only those disruptions to systems connected to OCC’s Systems, whether via an established communication channel from a Clearing Member, or through the Clearing Member’s Third-Party Service Provider; it is not intended to capture every disruption to every system of the Clearing Member or its Third-Party Service Provider. In addition, as described in further detail in section (d) of proposed Rule 213, OCC proposes to eliminate the existing definition of a “Security Incident” to remove language that invites Clearing Members to assess the potential impact of such incident on OCC’s Systems and operations when determining whether an incident is reportable. OCC’s existing definition of a “Security Incident,” is defined, in part, as an incident, or an incident that is occurring, involving a cyber-related disruption or intrusion of the Clearing Member’s systems that is reasonably likely to pose an imminent risk or threat to OCC’s operations. OCC believes the language in the existing definition invites Clearing Members to assess whether such incident to their systems would impact OCC, and therefore OCC proposes to eliminate the definition of “Security Incident” and replace the definition with “Clearing Member System Event” in proposed Rule 213.

- Define “OCC’s Systems” to mean the systems, equipment and technology networks of OCC, whether owned, leased, or licensed, and including software, hardware, applications, devices, IP addresses, or other addresses or accounts used in an established communication channel with such systems, equipment and technology networks, to provide the services set forth in these Rules, or otherwise used to transact business or connect with OCC. OCC proposes to introduce the definition of “OCC’s Systems” for the purposes of Rule 213 to articulate OCC’s potentially impacted connections and any means of connectivity in the event of a Clearing Member System Event. OCC’s proposed definition incorporates not only direct connections but also references “established communication channels,” which OCC believes may include access to File Transfer Protocol (“FTP”) for transmitting data or instructions that may be compromised by a systems intrusion to a Clearing Member’s back-office systems.
- Define a “Major Clearing Member System Event” to mean a Clearing Member System Event that has or is reasonably anticipated to, for example, disrupt, degrade, cause a delay in, interrupt or otherwise alter the normal operation of OCC’s Systems; result in unauthorized access to OCC’s Systems; result in the loss of control of, disclosure of, or loss of OCC’s Confidential Information; or cause a strain on, loss of, or overall threat to the OCC’s resources, functions, security or operations. The purpose of establishing the concept of a “Major Clearing Member System Event,” is to tie the disruption at issue to its effect on the normal operations of OCC. This concept introduces a threshold level in which OCC would be authorized to take action, including disconnection, in the event OCC determines that a Clearing Member

System Event rises to the level of a Major Clearing Member System Event.¹⁰ OCC believes the concept of a “Major Clearing Member System Event” will strengthen OCC’s security protocols by establishing a baseline by which OCC can measure the disruption at issue against its impact on OCC and, as described in further detail below, take action to mitigate risks presented.

- Define “Third-Party Cybersecurity Firm” to mean a firm that, in OCC’s reasonable judgement, (A) (i) is well-known and reputable; (ii) is not the subject Clearing Member, or an affiliate or a Third-Party Service Provider of the subject Clearing Member; (iii) is experienced in financial-sector cybersecurity; and (iv) employs Best Practices; or (B) is otherwise determined to be a Third-Party Cybersecurity Firm by OCC. OCC proposes to include this definition to clearly describe the type of firm that OCC would require the subject Clearing Member to engage under proposed Rule 213(g)(3).
- Define “Third-Party Service Provider” to mean an affiliate of any Clearing Member, service bureau or other similar entity, that connects to OCC’s Systems on behalf of or for the benefit of a Clearing Member. This proposed definition would help clarify that OCC Rule 213 applies to a Clearing Member’s Third-Party Service Provider’s connections to OCC’s Systems.

Proposed Rule 213(b) – Cybersecurity Confirmation Submission

Proposed Rule 213(b) incorporates the provision from existing Rule 213(a)(ii) into proposed Rule 213(b)(1) to promote clarification and efficiency. Proposed Rule 213(b) also

¹⁰ OCC’s Information Security Disconnect and Reconnect Procedure is contained in Confidential Exhibit 3 of SR-OCC-2026-010, and it outlines how OCC determines that a Clearing Member System Event rises to the level of a Major Clearing Member System Event.

makes other conforming and non-substantive changes, including reorganizing provisions into a hierarchical structure, and updating language to promote clarity and efficiency.

Existing Rule 213(a) requires Clearing Members and clearing membership applicants to periodically submit a form, provided by OCC, confirming, in part, that they have a cybersecurity program in place (“Cybersecurity Confirmation”). Sections (i) and (ii) of existing Rule 213(a) require that applicants must submit it with their application, and existing Clearing Members must resubmit it at least every two years, within 180 days of the OCC’s notice requiring attestation. OCC’s proposed changes streamline existing Rule 213(a) into proposed Rule 213(b)(1) by combining the general description of the Cybersecurity Confirmation requirement with the specific timing obligation applicable to Clearing Members into a single paragraph. Specifically, OCC’s proposed Rule 213(b)(1) would provide, in part, that each Clearing Member must complete and submit “an attestation at least every two years, and not later than 180 calendar days from the date that OCC notifies the Clearing Member that the attestation is required.” In addition, proposed Rule 213(b)(1) would remove the reference to the phrase “applicant for clearing membership” as OCC believes such language is duplicative since it is included in the subsequent provision in proposed Rule 213(b)(2). OCC’s proposed changes replace the term “shall” with “must” in proposed Rule 213(b)(1) and proposed Rule 213(b)(2) to promote stronger cadence and readability. OCC’s proposed changes also eliminate the specific reference to the word “form” after “attestation.” The concept of a “form” and an “attestation” may introduce different meanings, so this proposed change is intended to eliminate ambiguity and maintain consistency with OCC’s referenced term, “Cybersecurity Confirmation.” OCC also proposes to eliminate the reference that the attestation is “provided by the Corporation” because

OCC believes this is unnecessary to specify. Finally, OCC proposes to remove the word “materials” in proposed Rule 213(b)(2) to promote efficiency.

Proposed Rule 213(c)¹¹ – Representations in the Cybersecurity Confirmation

OCC’s proposed changes relocate the signature requirement set forth in existing Rule 213(c), “Execution of the Cybersecurity Confirmation,” into the introductory provision of proposed Rule 213(c), “Representations in the Cybersecurity Confirmation” (redesignated from existing Rule 213(b)). As relocated, the requirement would provide that the Cybersecurity Confirmation must be signed by a senior executive of the Clearing Member or applicant who is authorized to attest to these matters, consistent with the substance of the existing requirement. Existing Rule 213(c) would be deleted in its entirety, as its sole requirement is preserved within proposed Rule 213(c). OCC believes this change is non-substantive and is designed to eliminate duplicative rule text and improve the clarity and organization of Rule 213. OCC’s proposed changes also remove the word “designated” from the signature requirement, such that the Cybersecurity Confirmation may be signed by any senior executive of the Clearing Member or applicant who is authorized to attest to these matters, rather than requiring a designated senior executive. Specifically, proposed Rule 213(c) would provide that the Cybersecurity Confirmation “must be signed by a senior executive of the Clearing Member or applicant who is authorized to attest to these matters.” OCC believes the term “designated” creates ambiguity. Additionally, OCC believes that removing this term improves operational flexibility by allowing any senior executive with the requisite authorization to sign and improves timely compliance by avoiding delays that could arise if a specifically designated individual is unavailable at the time attestation is required. OCC believes the proposed change preserves the integrity and reliability

¹¹ Existing Rule 213(b) would be renumbered to proposed Rule 213(c).

of the attestation, since the signatory must still be a senior executive with the requisite authorization to attest to these matters.

OCC's proposed changes to Rule 213(c) also make other non-substantive changes, including reorganizing the provisions into a hierarchical structure and replacing the term "shall" with "must" to promote stronger cadence and readability.

Proposed Rule 213(d) – Occurrence of a Clearing Member System Event

OCC's proposed Rule 213(d) would introduce enhanced notification requirements for a Clearing Member in the event of a Clearing Member System Event. More specifically, OCC's proposed changes would introduce a particular timeframe required for Clearing Members to report such incident and specify the information that must be included in the notification.

First, as referenced above in the proposed "Defined Terms" section, OCC proposes to re-define and broaden the definition of "Security Incident" to "Clearing Member System Event." In alignment with this proposed change, OCC would also eliminate the existing definition of a "Security Incident" in proposed Rule 213(d), which states in part, that such incident is one that is occurring involving a cyber related disruption or intrusion of the Clearing Member's systems that is reasonably likely to pose an imminent risk or threat to OCC's operations.

Second, OCC's proposed changes would require that a Clearing Member experiencing a Clearing Member System Event must notify OCC immediately "in writing, but no later than two hours" after the Clearing Member becomes aware or should be aware that there has been a Clearing Member System Event. The purpose of including a specific timeframe of two hours for which a Clearing Member System Event must be reported is to clarify OCC's existing standard of "immediate" in order to help mitigate the risk presented by a Clearing Member or its Third-

Party Service Provider that is experiencing such incident.¹² OCC believes that the term “immediately,” standing alone, may be interpreted differently and therefore could create uncertainty and inconsistent compliance. By pairing “immediately” with a definite, objective two-hour limit, OCC’s Clearing Members will have a clear, unambiguous benchmark for timely notification. By receiving notification of a Clearing Member System Event within two hours of its occurrence, OCC believes it will be able to address and respond to such event in a timely manner and take proactive steps to reduce any future risk presented to OCC and its Clearing Members. If a Clearing Member does not report a Clearing Member System Event within the notification timeframe set forth in section (d), OCC will evaluate the facts and circumstances of the delay in notification to determine whether a rule violation has occurred that is subject to OCC’s disciplinary process under Chapter XII of OCC’s Rules.

Third, OCC’s proposed changes require that notification of proposed section 213(d) must, at a minimum include the following information (as described below), and any such information unconfirmed or otherwise unknown may be identified by the Clearing Member as “Unknown.” OCC’s existing Rule 213 does not expressly set out requirements for what to include in a notification of a Clearing Member System Event. While OCC already obtains the required information outlined out in proposed Rule 213(d) through its existing practice, the required information is not memorialized in OCC’s Rules, policies, or procedures. This practice has historically included, among other things, requests regarding the legal entity name of the Clearing Member, contact information of individuals authorized to act on its behalf, and key details of the incident such as its nature, status, systems or data affected, and remediation steps

¹² OCC’s current rule 213(d) requires a member to immediately notify OCC and to confirm such notice promptly in writing.

taken. OCC typically obtains this information from the Clearing Member via phone or email, depending on the circumstances. This information is generally gathered over the course of OCC's engagement with the Clearing Member as the incident develops and the Clearing Member's own understanding of the incident evolves, rather than all at once at the onset of the incident. As such, the purpose of proposed section 213(d) is to codify what OCC already expects in practice, so that all Clearing Members are aware, in advance, of the information required to be included when reporting a Rule 213 incident.

OCC's proposed changes provide that the information required to be in the notice, if known, include: (i) the legal entity name of the Clearing Member or its Third-Party Service Provider affected by the Clearing Member System Event, (ii) contact information of individuals who are authorized to act on behalf of the subject Clearing Member regarding the Clearing Member System Event, and (iii) key details of the Clearing Member System Event such as event type, event effect, start date, end date, discovery date, scope, and any other notices given that would help to provide additional context of the Clearing Member System Event. As discussed above, OCC's existing Rule 213 does not expressly set out requirements for what information must be included in a notification of a Clearing Member System Event. In practice, OCC would obtain the same details identified in proposed section 213(d), but not all at once and not in the formal manner that proposed section 213(d) establishes.

OCC's proposed changes to Rule 213(d) would provide that the information required in the notice related to "Legal Entities" would include a complete list of the legal entity names of the Clearing Member and any Third-Party Service Providers experiencing or otherwise affected or potentially affected by the Clearing Member System Event. In addition, OCC's proposed changes would require that information required in the notice related to "Contact Information"

would include list of persons – with their corresponding titles, primary email addresses and phone numbers, and if those primary email addresses and phone numbers are associated with the systems that are the subject of the Clearing Member System Event, alternate email addresses and phone numbers – who are authorized to act on behalf of the subject Clearing Member regarding the Clearing Member System Event. Furthermore, OCC’s proposed changes would provide that information required in the notice related to “Clearing Member System Event Details” would include requirements in sections (A) through (G) of proposed Rule 213(d):

(A) Event Type – the type of Clearing Member System Event, for example an insider threat, phishing attack, Man-in-the-Middle (“MITM”)¹³ attack, privilege escalation, denial of service, external threat, malware, unauthorized access, ransomware, compromised user account, SQL injections, brute force attack, system compromise, supply chain attacks (as each term is commonly understood by cybersecurity professionals in the financial sector), or other with a provided explanation;

(B) Event Effect – perceived, anticipated, or known effect of the Clearing Member System Event, for example, loss of communication, data corruption, security breach, or other with a provided explanation;

(C) Start Date – date and time when the Clearing Member System Event began;

(D) End Date – date and time when the Clearing Member System Event ended, if applicable;

(E) Discovery Date – date and time when the Clearing Member System Event was first

¹³ A man-in-the-middle (“MITM”) attack is an attack in which an adversary positions itself between two communicating parties in order to intercept and alter the data traveling between them. See National Institute of Standards and Technology, Computer Security Resource Center, Glossary, Man-in-the-Middle Attack (MitM), https://csrc.nist.gov/glossary/term/man_in_the_middle_attack.

identified;

(F) Scope – scope of the Clearing Member System Event, including, but not limited to, a list of each affected or likely affected system or data, including OCC’s Systems and data, the degree of such affect, and any supporting evidence of such; and

(G) Notices – whether any formal or informal notices or information regarding the Clearing Member System Event was made public and, if so, provide a copy of such notices or information.

The purpose of these proposed changes is to codify OCC’s expectations to increase transparency around OCC’s existing process. More specifically, OCC’s proposed changes codify, within Rule 213(d), the information that OCC has historically requested from Clearing Members during a Rule 213 event. Currently, OCC receives this information from Clearing Members upon request during a Rule 213 event as an incident unfolds, rather than receiving a standardized set of information upfront. By codifying OCC’s expectations directly in this Rule, OCC intends to increase transparency and ensure that all Clearing Members know, in advance, precisely what information they must provide when reporting a Rule 213 incident, as well as the types of information OCC may request as its investigation proceeds. OCC believes this advance clarity will enable Clearing Members to prepare more effectively and will allow OCC to more promptly and effectively review and mitigate any risk associated with the incident.

OCC believes that the requested information in the proposed sections (A) through (G), including Legal Entities, Contact Information, and details of the Clearing Member System Event are essential pieces of information that would help OCC to efficiently and effectively review and take action to mitigate risk presented. OCC also believes the proposed changes will allow Clearing Members and their Third-Party Service Providers to better understand and prepare for

their obligations to OCC in the event they experience a Clearing Member System Event.

Proposed Rule 213(e)¹⁴ – Declaration of a Major Clearing Member System Event

OCC proposes to introduce new Rule 213(e) sections (1) through (3), which would focus on the declaration of a Major Clearing Member System Event, including the details surrounding who is authorized to declare such event and notification requirements associated with such event.

First, proposed Rule 213(e)(1) would provide that upon becoming aware of a Clearing Member System Event, OCC will consider whether such Clearing Member System Event meets the definition of a Major Clearing Member System Event. The proposed change would also provide that the existence of a Major Clearing Member System Event must be declared by two or more Designated Officers of OCC, in their reasonable judgement.

Second, proposed Rule 213(e)(2) would provide that upon declaration of a Major Clearing Member System Event, OCC may act (or refrain from acting) pursuant to this Rule to help address, correct, mitigate or alleviate any and all risks presented to OCC by or related to the Major Clearing Member System Event. The proposed change would also provide that action taken will be in consideration of the risks presented to OCC, including but not limited to, information provided pursuant to this Rule.

The purpose of OCC's Proposed Rule 213(e)(1) through (2) is to clarify that OCC will assess the potential impact of a Clearing Member System Event on OCC's Systems and operations, and OCC will determine to act, or refrain from acting, depending on the details of the Clearing Member System Event. The proposed rule removes any ambiguity that may exist in present language that invites the Clearing Member to assess potential impact of the Clearing Member System Event on OCC's Systems or operations. The purpose of the proposed change is

¹⁴ Existing Rule 213(e) would be renumbered to Rule 213(g).

also to clearly define who is authorized to declare a Major Clearing Member System event, specifically, that such a declaration must be made by two or more Designated Officers of OCC. OCC believes it is appropriate that such declaration be made by two or more Designated Officers of OCC to ensure that information regarding the Clearing Member System Event has been escalated to and considered at the highest management level. OCC believes the proposed rule change also provides transparency to Clearing Members and other stakeholders as to who is authorized to declare a Major Clearing Member System Event.

Lastly, OCC's proposed changes introduce a new requirement that OCC notify the Chairman of the Board of Directors following a declaration of a Major Clearing Member System Event. Specifically, proposed Rule 213(e)(3) provides that following declaration of a Major Clearing Member System Event, OCC will promptly notify the Chairman of the Board of Directors of such declaration. Because a Major Clearing Member System Event reflects OCC's determination that a Clearing Member System Event may have a significant impact on OCC's Systems or operations, OCC believes it is appropriate that this information be escalated to the Chairman of the Board of Directors without delay. OCC believes that notifying the Chairman is appropriate because it allows the Chairman to determine, based on the nature and severity of the specific Major Clearing Member System Event, the extent to which the full Board or any relevant Board Committee should be further notified or involved.

Proposed Rule 213(f) – Authority to Take Action and Required Cooperation

Proposed Rule 213(f) would expand upon OCC's existing authority to take action in the event of a Clearing Member System Event and associated Major Clearing Member System Event. More specifically, proposed Rule 213(f) introduces requirements surrounding: (i) OCC's ability to act, or refrain from acting, in the event of a Major Clearing Member System Event, (ii)

OCC's responsibility to notify the Clearing Member of any disconnect or material action taken, and (iii) the Clearing Member's responsibility to cooperate fully and to the reasonable satisfaction of OCC in the event of a Major Clearing Member System Event. Proposed Rule 213(f) also makes other conforming and non-substantive changes, including reorganizing provisions into a hierarchical structure, and updating language to promote clarity and efficiency.

OCC's proposed changes would organize Rule 213(f) into subsections (1) through (4). Proposed Rule 213(f)(1) details, in part, OCC's ability to, in the event of a Clearing Member System Event, take actions reasonably necessary to mitigate any impact to its operations, including actions described in proposed Rule 213(f)(1)(A) through Rule 213(f)(1)(C).¹⁵ OCC's changes to proposed Rule 213(f)(1)(A) make conforming and non-substantive changes to the text, including removing the phrase "the right to." To maintain consistency and align with OCC's proposed definition of OCC's Systems, OCC proposes to eliminate the term "data" before systems in proposed Rule 213(f)(1)(A). Proposed Rule 213(f)(1)(B) is new and provides that OCC may take actions reasonably necessary to mitigate any effects to its operations, including to suspend any and all transmissions, communications, or access between OCC's Systems (together with actions taken under Rule 213(f)(1)(A), "disconnect"). The purpose of this change is to broaden OCC's authority to take action that OCC believes may be necessary to mitigate risk presented by a Clearing Member System Event and associated Major Clearing Member System Event. In addition to OCC's existing authority to disconnect access of a Clearing Member, as described in proposed Rule 213(f)(1)(A), OCC believes the proposed change to expand OCC's authority to suspend any and all transmission, communication or access of a Clearing Member

¹⁵ The proposed changes would not substantively alter this section of 213(f) but include only conforming changes such as changes to match defined terms.

will help to ensure that OCC can adequately address all potential connectivity and communication types of a Clearing Member. OCC also proposes to adopt new Rule 213(f)(1)(C) to provide OCC the authority to act in the event OCC determines that a Major Clearing Member System Event has occurred. Proposed Rule 213(f)(1)(C) provides that OCC may take, or refrain from taking, or require the subject Clearing Member to take or refrain from taking, any and all action that OCC considers appropriate to help address, correct, mitigate or alleviate the Major Clearing Member System Event and, as appropriate and practical, facilitate the continuation of services, which may include issuing instructions to the subject Clearing Member and requiring such Clearing Member to act on such instructions. Examples of actions that OCC considers appropriate may include, but are not limited to, disconnection from OCC's Systems, forced password resets, and requiring the Clearing Member to use alternative communication and file transfer methods (e.g. secure file transport instead of email). The purpose of this proposed change is to provide OCC with the authority to evaluate and address a Major Clearing Member System Event and adequately respond to such event in effort to mitigate impact to OCC and its Clearing Members. Additionally, in the event OCC determines a Major Clearing Member System Event has occurred, by adding the provision that allows OCC to issue instructions and requires the subject Clearing Member to follow those instructions, OCC believes this requirement will help to help facilitate the continuation of services for the subject Clearing Member and alleviate future impact that may otherwise result from the disruption. Specifically, the issuance of instructions allows OCC to direct a more tailored response that is specific to the nature and severity of the Major Clearing Member System Event. This flexibility enables OCC to address the risk presented by a specific Major Clearing Member System Event while, where

practicable, preserving the Clearing Member's ability to continue some or all of its services during remediation.

OCC proposes to adopt Rule 213(f)(3), which addresses OCC's notification requirements to the Clearing Member, as well as the subject Clearing Member's obligations to comply with OCC's statutory rules. More specifically, proposed Rule 213(f)(3) would provide that OCC will promptly notify the Clearing Member of any disconnect or other material action that OCC takes with respect to such Clearing Member pursuant to Rule 213. In addition, proposed Rule 213(f)(3) would provide that, notwithstanding any action taken pursuant to Rule 213, the Clearing Member must continue to meet its obligations to OCC and comply with OCC's statutory rules, as defined in its By-Laws. Under OCC's existing Rule 213, if OCC determines that disconnection of a Clearing Member from OCC's Systems is necessary, the Clearing Member must continue to meet its obligations to OCC notwithstanding that disconnection. OCC's existing Rule 213(d) focuses solely on the Clearing Member's continuing obligations following a disconnection and it does not address whether OCC will notify the Clearing Member that a disconnection (or any other action) has occurred. Proposed Rule 213(f)(3) expands the current provision in two respects: (i) it adds a notification obligation on OCC's part, and (ii) it broadens both the scope of triggering actions (from disconnection alone to any material action under the Rule) and the scope of the Clearing Member's continuing obligations to also include compliance with OCC's statutory rules, as the term is defined in OCC's By-Laws.

These proposed changes serve several purposes. First, the purpose of requiring OCC to promptly notify a Clearing Member of any disconnection or other material action taken under this Rule is to provide enhanced transparency to Clearing Members regarding actions that OCC takes that impact them. OCC believes it is prudent to notify the Clearing Member promptly in

such event to allow the Clearing Member to better prepare for and understand their obligations to OCC. Second, the proposed change expands the scope of that notification obligation from disconnection alone to “any material action” taken pursuant to the Rule. This may include, for example, modifying the scope and specifications of access of the Clearing Member to OCC’s Systems. The purpose of this proposed change is to ensure that Clearing Members receive notice of any material action OCC may take, not solely the most severe action of disconnection. Third, the proposed change broadens the Clearing Member’s continuing obligations to apply “notwithstanding any action taken pursuant to this Rule,” rather than only “notwithstanding disconnection,” removing any ambiguity as to whether a Clearing Member’s obligations to OCC continue in the event OCC takes a material action, outside of disconnection. Finally, the proposed change also specifies what obligations the Clearing Member must continue to meet, by adding an express requirement that the Clearing Member comply with the statutory rules of OCC, as defined in OCC’s By-Laws. OCC’s current Rule 213 refers only generally to the Clearing Member’s “obligations to OCC” without specifying what those obligations include. OCC believes the addition of “comply with the statutory rules of OCC, as defined in its By-Laws” clarifies what those obligations encompass. OCC’s proposed changes to proposed Rule 213(f)(3) also make other conforming, non-substantive changes.

Lastly, OCC proposes to adopt new Rule 213(f)(4), which requires that the Clearing Member must cooperate fully and completely with, and to the reasonable satisfaction of, OCC in all matters relating to the Major Clearing Member System Event, including, but not limited: (i) conducting timely investigations and inquiries, as OCC believes reasonably necessary, with respect to any known or unknown information relating to the Clearing Member System Event; (ii) promptly notifying OCC of any material changes, updates, or new information learned

regarding the Clearing Member System Event; and (iii) promptly providing any documentation or information requested by OCC, unless not legally permitted to do so, regarding or related to the Clearing Member System Event.¹⁶ The purpose of this proposed change is to provide enhanced transparency to Clearing Members on their obligations to comply with the proposed requirements. OCC believes that cooperation from Clearing Members on matters relating to a Major Clearing Member System Event will help OCC to efficiently and effectively manage and respond to a Major Clearing Member System Event in effort to mitigate risk presented.

Proposed Rule 213(g)¹⁷ Procedures for Reconnection

OCC proposes to update existing Rule 213(e) titled “Procedures for Connecting Following a Security Incident that Results in Disconnection” to Proposed Rule 213(g) titled “Procedures for Reconnection.” OCC believes that such change in title is necessary to more accurately encompass the obligations of a Clearing Member pursuant to OCC’s authority to act in the event of a Clearing Member System Event, as described in proposed Rule 213(f)(1). The retitled rule sets forth the information that the subject Clearing Member would be required to provide OCC in the event OCC takes action pursuant to proposed Rule 213(f)(1) and includes both substantive and non-substantive changes as described below. Proposed Rule 213(g) also reorganizes existing Rule 213(e) into proposed Rule 213(g)(1) through 213(g)(2), and incorporates new section (3) in proposed Rule 213(g)(3) titled “Report from Third-Party Cybersecurity Firm.”

Proposed Rule 213(g)(1) Reconnection Attestation

OCC’s proposed Rule 213(g)(1) would be titled “Reconnection Attestation.” Proposed

¹⁶ Sections (i) through (ii) described in the narrative would be numbered to proposed Rule 213(f)(4)(A) though proposed Rule 213(f)(4)(C).

¹⁷ Existing Rule 213(e) would be renumbered to proposed Rule 213(g).

Rule 213(g)(1) would include the current requirement that a subject Clearing Member must complete and submit a Reconnection Attestation prior to OCC reestablishing connectivity to OCC's Systems. More specifically, proposed Rule 213(g)(1) would provide that if OCC takes action pursuant to Rule 213(f)(1), the Clearing Member must complete and submit a form as provided by OCC that describes the Clearing Member System Event and includes required representations ("Reconnection Attestation"). OCC proposes to add language to clarify that such requirement must be met prior to OCC reestablishing connectivity to OCC's Systems ("Reconnection"). OCC proposes to relocate the existing provision that states "The Clearing Member also will be required to complete an associated checklist provided by OCC that describes remediation efforts ("Reconnection Checklist")," because OCC believes such text is more appropriately located in proposed Rule 213(g)(2), which outlines the requirements in the Reconnection Checklist. In addition, OCC's proposed changes collapse and consolidate Rule 213(e)(1) into Rule 213(e), which becomes proposed Rule 213(g), such that the signature requirement is now reflected in proposed Rule 213(g)(1). Specifically, OCC's proposed changes reflect that the provision in current Rule 213(e)(1) on the requirement for the Reconnection Attestation to be signed by a designated senior executive becomes included in proposed Rule 213(g)(1). This change is intended to make Rule 213 easier to navigate by grouping related requirements together; it does not alter the Clearing Member's underlying obligation to obtain a signature from an individual who maintains the authorization to sign the Reconnection Attestation. OCC's proposed changes also eliminate the term "designated" when describing the senior executive of the Clearing Member that must sign the Reconnection Attestation. OCC believes the term "designated" creates ambiguity. By removing this term, OCC believes it

improves operational flexibility by allowing any senior executive of the Clearing Member¹⁸ with the requisite authorization to sign, and it improves timely compliance by avoiding delays that could arise if a specifically designated individual is unavailable at the time attestation is required. OCC believes the proposed change preserves the integrity and reliability of the attestation, since the signatory must still be a senior executive with the requisite authorization to attest to these matters.

In addition, proposed Rule 213(g)(1)(A) through 213(g)(1)(E) incorporates the requirements in current Rule 213(e)(1)(A) through Rule 213(e)(1)(E) and makes other non-substantive changes including renaming the term “Security Incident” to “Clearing Member System Event,” as described in proposed Rule 213(a).

Proposed Rule 213(g)(2) Reconnection Checklist

OCC’s proposed Rule 213(g)(2) would be titled “Reconnection Checklist.” Proposed Rule 213(g)(2) reorganizes the provisions from existing Rule 213(e)(2) into proposed Rule 213(g)(2) and subsections (A) through (J) of proposed Rule 213(g)(2) to promote clarity and efficiency. OCC’s proposed changes also make other conforming, clarifying and non-substantive changes. More specifically, OCC’s proposed changes to Rule 213(g)(2) provide that if OCC takes action pursuant to Rule 213(f)(1), the Clearing Member must complete an associated checklist as provided by OCC that describes remediation efforts (“Reconnection Checklist”), which may require information including but not limited to the information in proposed

¹⁸ A senior executive of the Clearing Member with the requisite authorization to sign may for example include, but is not limited to, a member of the board of directors or a member of senior management with the requisite knowledge and experience to make such an attestation, as determined by the Clearing Member’s own delegation of authority and procedures.

subsections (A) through (J) of proposed Rule 213(g)(2).

Proposed Rule 213(g)(3) Report from Third-Party Cybersecurity Firm

OCC proposes to adopt Rule 213(g)(3), titled “Report from Third-Party Cybersecurity Firm,” which provides that OCC may require that the subject Clearing Member provide a report from a Third-Party Cybersecurity Firm, either as a condition to Reconnection or following Reconnection. OCC’s proposed changes describe the information required to be in such report in proposed Rule 213(g)(3)(A) through proposed Rule 213(g)(3)(G).

More specifically, proposed Rule 213(g)(3) states that if OCC takes action pursuant to Rule 213(f)(1), OCC may require, either as a condition to reconnection or following reconnection, that the Clearing Member provide a detailed, comprehensive, and auditable report from a Third-Party Cybersecurity Firm, or a summary of such report that includes: (i) a timeline of the Clearing Member System Event, including all material actions, events, and decisions taken for or relating to the Clearing Member System Event; (ii) a description of the Clearing Member System Event and an explanation of how such disruption was corrected or resolved; (iii) root cause analysis of the Clearing Member System Event; (iv) confirmation that any issues identified by the Third-Party Cybersecurity Firm as severe, critical, or moderate, or comparable categorizations, have been resolved; (v) confirmation of normal or intended operation of the subject system(s), including, but not limited to, the return or replacement of key systems and data stores to pre-Clearing Member System Event resilience, in a safe, secure and proper manner for at least 72 hours; (vi) a description of short-and long-term preventive monitoring and detection recommendations from the Third-Party Cybersecurity Firm; and (vii) any other information

reasonably requested to be included by OCC.¹⁹ In the event a Clearing Member is the subject of action pursuant to OCC's authority under proposed Rule 213(f)(1), the purpose of proposed Rule 213(g)(3) is to provide OCC with all necessary information about the subject Clearing Member's disruption and its remediation from an independent, knowledgeable and reputable Third-Party Cybersecurity Firm, so that OCC can determine whether Reconnection is appropriate. OCC's ability to require an audit report from a Third-Party Cybersecurity Firm provides OCC with essential information that will help OCC to fully evaluate the Clearing Member System Event and take steps to mitigate risks presented by such incident.

Proposed Rule 213(h) Reconnection Testing and Approval

OCC's proposed changes would adopt Rule 213(h) titled "Reconnection Testing and Approval," which would require, prior to any Reconnection, that the subject Clearing Member must demonstrate, as applicable, to OCC's reasonable satisfaction, that it: (i) can operate in a test environment, including, but not limited to, sending and receiving messages and transactions; (ii) can replay or resubmit previously submitted messages or transactions; (iii) can reverse or void previously submitted messages or transactions; (iv) can confirm the integrity of messages and transactions; (v) has alternative communication methods with OCC to facilitate the exchange of messages, transactions, and reports; and (vi) can complete any other such requirements as are reasonably requested by OCC. Furthermore, proposed Rule 213(h)(2) would authorize two or more Designated Officers of OCC to, in their reasonable judgment, approve the Reconnection of a Clearing Member that was the subject of action taken pursuant to proposed Rule 213, after OCC has received all required information pursuant to this Rule, in a form and a substance

¹⁹ The provisions described in subsections (i) through (vii) above would be organized as subsections (A) through (G), respectively, in proposed Rule 213(g)(3).

satisfactory OCC, and that all information necessary for a safe Reconnection and certain testing has occurred, pursuant to proposed Rule 213(h)(1).

The purpose of proposed Rule 213(h) is to ensure that the approval for a Reconnection is not made until OCC has received, to its satisfaction, all necessary information from the Clearing Member, and that OCC confirmed the subject Clearing Member can safely perform the capabilities necessary for submitting, receiving, and correcting information appropriately and in a manner unaffected by the Clearing Member System Event, so as to help mitigate the risk presented by the Reconnection. In addition, OCC believes it is appropriate that the approval of a Reconnection be made by at least two members of OCC's management committee to help ensure that information regarding the Reconnection has been escalated to the highest management level.

Proposed Rule 213(i) Certain Miscellaneous Matters

OCC proposes to adopt Rule 213(i), titled "Certain Miscellaneous Matters," which would address various provisions including, but not limited to, (i) OCC's limited liability to a Clearing Member pursuant to proposed Rule 213; (ii) OCC's authority to inform the subject Clearing Member's Third-Party Service Provider, or require the Clearing Member to inform its Third-Party Service Provider, of a Clearing Member System Event; and (iii) the failure of a Clearing Member to comply with proposed Rule 213.

First, in an effort to promote enhanced transparency to Clearing Members, proposed Rule 213(i)(1) would address, in part, OCC's limited liability to any Clearing Member as it relates to losses arising out of OCC's action or inaction pursuant to proposed Rule 213. More specifically, proposed Rule 213(i)(1) would provide that without limiting any other provisions in these Rules concerning limitations on liability, neither OCC nor its directors, officers, employees, agents, or contractors shall be liable to any Clearing Member or any customer or client thereof for: (i) any

failure, hindrance, interruption or delay in performance in whole or in part of the obligations of OCC under these Rules, if that failure, hindrance, interruption or delay arises out of or relates to a Clearing Member System Event, Major Clearing Member System Event, or any action or inaction pursuant to this Rule 213; or (ii) any loss, liability, damage, cost or expense arising from or relating in any way to any advice, request, requirement, instruction, action or inaction pursuant to this Rule 213.²⁰ Second, proposed Rule 213(i)(2) would provide that the power of OCC to take any action pursuant to this Rule 213, or to request or require any action, documentation, or information pursuant to this Rule 213, also includes the power to waive, repeal, rescind, revoke, amend, or vary any such action, request, or requirement in consideration of the facts and circumstances. Third, proposed Rule 213(i)(3) would provide that the powers of OCC pursuant to this Rule 213 are in addition to, and not in limitation of, any authority granted elsewhere in these Rules to act as specified therein. The purpose of proposed Rule 213(i)(2) and proposed Rule 213(i)(3) is to promote enhanced transparency to Clearing Member on OCC's authority to take action pursuant to Rule 213 so that Clearing Members can better understand and be prepared for their obligations to OCC.

Fourth, proposed Rule 213(i)(4) would provide that all information related to or regarding a Major Clearing Member System Event and all acts pursuant to this Rule 213 will be considered Confidential Information pursuant to these Rules; provided, however, that the OCC may inform, or direct the Clearing Member to inform, the Clearing Member's Third-Party Service Provider of a Clearing Member System Event if OCC determines, in its discretion, that such action is necessary for the protection of OCC and other Clearing Members. The purpose of

²⁰ The provisions described in (i) through (ii) would be organized as proposed Rule 213(i)(1)(A) through 213(i)(1)(B).

the proposed change is to mitigate risk to OCC and its Clearing Members that may be presented by a Clearing Member System Event and associated Major Clearing Member System Event. The proposed changes also provide transparency to Clearing Members on their obligation to inform their Third-Party Service Providers in certain circumstances that OCC deems necessary.

Fifth, proposed Rule 213(i)(5) would provide that the failure of a Clearing Member to comply with the requirements of this Rule 213 may subject the Clearing Member to any and all disciplinary action permitted under these Rules, including, without limitation, suspension. Lastly, proposed Rule 213(i)(6) would provide that a Clearing Member that has authorized another party, such as a Third-Party Service Provider, to access and use OCC's systems will be responsible for such authorized party's compliance with the requirements of this Rule 213 and any compliance failure by that authorized party will be deemed to be a failure of the authorizing Clearing Member. The purpose of proposed Rules 213(i)(5) and 213(i)(6) is to highlight the importance of complying with proposed Rule 213 and the actions OCC may take if there is a failure to comply.

B. Statutory Basis

OCC believes the proposed rule change is consistent with Section 17A of the Exchange Act²¹ and Rule 17ad-22(e)(2) and (e)(17)²² thereunder. Section 17A(b)(3)(F) of the Act²³ requires, among other things, that the rules of a clearing agency be designed to promote the prompt and accurate clearance and settlement of securities transactions, and to assure the safeguarding of securities and funds which are in the custody or control of the clearing agency or

²¹ 15 U.S.C. 78q-1.

²² 17 CFR 240.17ad-22(e)(2) and (e)(17).

²³ 15 U.S.C. 78q-1(b)(3)(F).

for which it is responsible. OCC's proposed amendments to Rule 213 are designed to help OCC assess and take appropriate action to manage the cybersecurity risks that may be introduced to OCC's Systems and information due to a Clearing Member System Event. The proposed changes to Rule 213 enhance OCC's processes to help mitigate risk and better protect OCC and its Clearing Members.

As described above, the proposed rule change would, in part: (i) introduce a defined terms section to Rule 213 that broadens the definition of OCC Systems to include established communication channels, such as FTPs, in addition to direct connections; (ii) require that the Cybersecurity Confirmation be signed by a senior executive of the Clearing Member or applicant who is authorized to attest to such matters; (iii) remove language inviting a Clearing Member to assess the potential impact of a Clearing Member System Event on OCC's systems and operations when determining whether the event is reportable, and instead specify the timeframe for reporting such an event and the specific information that must be included in the notice; (iv) establish the concept of a "Major Clearing Member System Event," including a declaration process requiring approval by two or more Designated Officers and prompt notification to the Chairman of the Board; (v) reorganize and clarify OCC's authority to take action in response to a Clearing Member System Event, including specifying the actions that constitute a "disconnect" and clarifying a Clearing Member's related obligations; (vi) add provisions establishing the reporting, testing, approval, and governance requirements necessary for reconnection, including OCC's ability to require an audit report from a Third-Party Cybersecurity Firm; and (vii) provide OCC with the authority to inform, or to require a Clearing Member to inform, the Clearing Member's Third-Party Service Provider of a Clearing Member System Event if OCC determines, in its discretion, that such action is necessary to protect OCC and other Clearing Members. OCC

believes that these proposed changes will enhance Rule 213 to be more efficient, effective and clear in the cybersecurity obligations of its Clearing Members so that OCC may better address cybersecurity risks to protect OCC and its Clearing Members. Among the amendments discussed above, OCC believes the following amendments to Rule 213 are particularly consistent with the requirements of Section 17A(b)(3)(F) of the Act, as discussed in further detail below: (i) expanded notification requirements applicable to a Clearing Member System Event; (ii) the establishment of the Major Clearing Member System Event and its related governance; and (iii) the process for Reconnection of a Clearing Member.

First, proposed Rule 213(d) codifies within OCC's rules the specific content and timeframe requirements for notification of a Clearing Member System Event, which OCC believes is consistent with the requirements of Section 17A(b)(3)(F) of the Act.²⁴ Under proposed Rule 213(d), a Clearing Member would be required to provide OCC with specified information at the onset of a Clearing Member System Event, including but not limited to the event type, effect, scope, start date, end date, discovery date, and any public notices related to the event. OCC believes this requirement will allow OCC to receive consistent, timely information from Clearing Members, which in turn, will help to minimize the risk that delayed or incomplete information impacts OCC's ability to respond promptly and effectively to such events. As such, OCC believes this proposed change supports the prompt and accurate clearance and settlement of securities transactions and assures the safeguarding of securities and funds that are in the custody or control of OCC, consistent with Section 17A(b)(3)(F) of the Act.²⁵

²⁴ Id.

²⁵ Id.

Second, proposed Rule 213(e) establishes the concept of a “Major Clearing Member System Event,” which OCC believes is also consistent with the requirements of Section 17A(b)(3)(F) of the Act.²⁶ Under proposed Rule 213(e), OCC would assess the potential impact of a Clearing Member System Event on OCC’s Systems and operations, and would determine to act, or refrain from acting, depending on the specific details of the event. This removes the ambiguity that may exist in the current rule text, which instead invites the Clearing Member to assess potential impact of its own Clearing Member System Event on OCC’s Systems or operations. Furthermore, under proposed Rule 213(e), the existence of a Major Clearing Member System Event must be declared by two or more Designated Officers of OCC, in their reasonable judgement. Following such a declaration, OCC will promptly notify the Chairman of the Board. OCC believes this process ensures that the most severe threats to OCC’s Systems and operations are escalated to the highest levels of OCC’s governance. OCC believes the establishment of a Major Clearing Member System Event and the governance outlined in proposed Rule 213(e) is consistent with Section 17A(b)(3)(F) of the Act because OCC, not the reporting Clearing Member, is best positioned to determine the severity of a threat to OCC’s own Systems and operations. Additionally, OCC believes that escalation to the highest levels of OCC’s governance helps to ensure events with the greatest potential impact to OCC receive attention and oversight proportionate to their severity. As such, OCC believes the proposed rule change is designed to assure the safeguarding of securities and funds in the custody or control of OCC, consistent with the requirements in Section 17A(b)(3)(F) of the Act.²⁷

²⁶ Id.

²⁷ Id.

Third, proposed Rule 213(h) establishes reconnection testing and approval requirements that OCC believes are consistent with Section 17A(b)(3)(F) of the Act. Under proposed Rule 213(h)(1), prior to Reconnection, a Clearing Member must demonstrate, to OCC's reasonable satisfaction, that it can, in part, operate in a test environment, send and receive messages and transactions, replay or resubmit previously submitted messages or transactions, reverse or void previously submitted messages or transactions, confirm the integrity of messages and transactions, and maintain alternative communication methods with OCC. These requirements test the Clearing Member's operational capability to interact accurately and reliably with OCC's Systems, rather than relying on the Clearing Member's representation that it is prepared to reconnect. OCC believes this proposed change is designed to safeguard securities and funds in the custody or control of OCC by verifying, before Reconnection occurs, that a Clearing Member's systems will not transmit corrupted or otherwise unreliable messages or transactions into OCC's Systems and operations. As such, OCC believes this proposed change is designed to assure the safeguarding of securities and funds in the custody or control of OCC, consistent with the requirements in Section 17A(b)(3)(F) of the Act.²⁸

Risks presented by a Clearing Member System Event could impact OCC's ability to clear and settle securities transactions, or to safeguard the securities and funds that are in its custody or control, or for which it is responsible. Therefore, by enhancing OCC's processes to mitigate these risks, including but not limited to: expanding the notification requirements, establishing the concept of a Major Clearing Member System Event, and enhancing its process for Reconnection, OCC believes the proposed changes would promote the prompt and accurate clearance and settlement of securities transactions and assure the safeguarding of securities and funds that are

²⁸Id.

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.²⁹

Consistency with Rule 17ad-22(e)(2)(i) and (v)

OCC believes the proposed changes to Rule 213 are consistent with Rule 17ad-22(e)(2)(i) and (v), which require, in part, that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to provide for governance arrangements that (i) are clear and transparent and (ii) specify clear and direct lines of responsibility.³⁰ OCC specifies in proposed Rule 213(e)(1) that the existence of a Major Clearing Member System Event must be declared by two or more Designated Officers of OCC, and OCC will provide notification of such declaration to the Chairman of the Board. Proposed Rule 213(e)(1) establishes a defined pathway from identification of the event, through declaration by two or more Designated Officers, to notification at the Board level. As such, OCC believes this specificity is consistent with the “clear and transparent” governance arrangements required by Rule 17Ad-22(e)(2)(i). It is likewise consistent with the “clear and direct lines of responsibility” required by Rule 17Ad-22(e)(2)(v), because this proposed change assigns responsibility for determining a Major Clearing Member System Event to a specifically identified group of officers.

Similarly, with respect to Reconnection, proposed Rule 213(h)(2) requires that the Reconnection of a Clearing Member following OCC’s action pursuant to proposed Rule 213(f)(1) be approved by two or more Designated Officers of OCC, and conditions that approval on OCC’s receipt of all information required under Rule 213, in a form and substance

²⁹ Id.

³⁰ 17 CFR 240.17ad-22(e)(2)(i) and (v).

satisfactory to OCC, and satisfaction of the applicable testing requirements set forth in proposed Rule 213(h)(1). By specifying both who is authorized to approve Reconnection and the steps that must be satisfied before that approval may be granted, proposed Rule 213(h)(2) establishes a transparent and structured approval process, consistent with Rule 17Ad-22(e)(2)(i). It also identifies, with the same specificity as the Major Clearing Member System Event declaration process, the officers responsible for making a determination to reconnect a Clearing Member, consistent with the clear and direct lines of responsibility required by Rule 17Ad-22(e)(2)(v). Therefore, OCC believes the proposed changes are consistent with Rule 17ad-22(e)(2)(i) and (v) under the Act.³¹

Consistency with Rule 17ad-22(e)(17)(i)

OCC believes the proposed changes to Rule 213 are also consistent with Rule 17ad-22(e)(17)(i) under the Act, which 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.³²

As described above, the proposed changes to Rule 213, in part: (i) enhance the requirements of Clearing Members to notify OCC in the event of a Clearing Member System Event; (ii) add provisions around reporting, testing and approval requirements, and governance necessary for Reconnection of a Clearing Member, in the event OCC takes action pursuant to

³¹ Id.

³² 17 CFR 240.17ad-22(e)(17)(i).

proposed Rule 213(f)(1); and (iii) update and add definitions for purposes of Rule 213 to clarify the obligations of a Clearing Members and its Third-Party Service Providers.

First, OCC believes the enhancements notification requirements in proposed Rule 213(d) are consistent with the requirements set forth in Rule 17Ad-22(e)(17)(i).³³ Proposed Rule 213(d) outlines the requirements applicable to a Clearing Member's notification of a Clearing Member System Event to OCC. This includes removing language that invites a Clearing Member to assess the potential impact of the event on OCC's Systems and operations in determining whether the event was reportable, specifying the timeframe within which such an event must be reported, and identifying the specific information that must be included in the notice. OCC believes these enhancements are consistent with Rule 17Ad-22(e)(17)(i), which requires OCC to identify the plausible sources of its operational risk, both internal and external. Because a Clearing Member System Event represents an external source of potential operational risk to OCC, OCC's ability to identify and characterize that risk depends on receiving timely, complete, and accurate information from the Clearing Member. The specified content requirements, including but not limited to, the event type, effect, scope, and start, end, and discovery dates, further support OCC's ability to identify the nature and extent of the risk presented. As such, OCC believes the proposed change helps OCC to identify, in a timely manner, plausible sources of operational risk presented by a Clearing Member System Event, and mitigate risk presented to OCC and its Clearing Members, consistent with Rule 17ad-22(e)(17)(i).³⁴

Second, OCC's proposed changes in Rule 213(h) enhance the requirements surrounding the Reconnection of a Clearing Member, which will help OCC evaluate and determine whether

³³ Id.

³⁴ Id.

Reconnection is appropriate and, if so, take steps to ensure a safe Reconnection. OCC believes these enhancements are also consistent with the requirements in Rule 17Ad-22(e)(17)(i) of the Act³⁵ that requires OCC to identify and mitigate the impact of its operational risks through appropriate systems, policies, procedures, and controls. Proposed Rule 213(h)(1) requires that, prior to Reconnection, a Clearing Member demonstrate, to OCC's reasonable satisfaction, that it can operate in a test environment, replay or resubmit previously submitted messages or transactions, reverse or void previously submitted messages or transactions, confirm the integrity of messages and transactions, and maintain alternative communication methods with OCC. OCC believes is consistent with the requirements in Rule 17Ad-22(e)(17)(i) because the proposed change identifies, through testing requirements, whether the specific risks presented by the original Clearing Member System Event, including, for example, data loss or communication failure, have been resolved. By requiring the Clearing Member to demonstrate these capabilities before Reconnection is granted, proposed Rule 213(h)(1) mitigates the risk that reconnecting the Clearing Member would reintroduce the same operational risk to OCC's Systems that necessitated the disconnection in the first place. In addition, under proposed Rule 213(g)(3), OCC can request a detailed, comprehensive, and auditable report from a Third-Party Cybersecurity Firm, either as a condition to or following Reconnection. This report must include, but is not limited to, a timeline of the Clearing Member System Event, a description of the event and how it was corrected or resolved, a root cause analysis, confirmation that any issues identified as severe, critical, or moderate have been resolved, confirmation that the affected systems have returned to normal, pre-incident operation for at least 72 hours, and short and long-term preventive monitoring and detection recommendations. OCC's ability to require an audit

³⁵Id.

report from a Third-Party Cybersecurity Firm will enable OCC to collect and evaluate information from a reputable source to help OCC determine whether to reconnect. The requirement for an independent root cause analysis supports OCC's identification of the operational risk's underlying cause, while the requirement for verified confirmation supports the rule's mitigation component. As such, OCC believes this proposed change is consistent with the requirements in Rule 17Ad-22(e)(17)(i).³⁶

Third, OCC believes the proposed addition of a defined terms section to Rule 213, including an expanded definition of OCC's Systems to encompass established communication channels, such as FTPs, that may be used to transmit data or instructions to a Clearing Member's back-office systems, is consistent with Rule 17Ad-22(e)(17)(i) of the Act.³⁷ OCC believes that expanding the definition of OCC's Systems to include these indirect channels is appropriate because a security intrusion can reach OCC through such a channel, in addition to a direct connection, so OCC believes it is prudent to codify this in its rules to help identify that potential source of risk. OCC's proposed changes also update the definition of a "Clearing Member System Event" to include an incident resulting from a Clearing Member's Third-Party Service Provider connected to OCC's Systems. By establishing definitions for these terms and, more specifically, expanding the definition of Clearing Member System Event to incorporate the Clearing Member's Third-Party Service Provider, this will help OCC to better identify and manage risks presented by a Clearing Member or its Third-Party Service Provider connected to OCC's Systems.

³⁶ Id.

³⁷ Id.

By enhancing reporting and notification requirements for Clearing Members in the event of a Clearing Member System Event, strengthening the testing, reporting, approval and governance requirements surrounding reconnection of a Clearing Member, and adding and updating definitions for the purpose of proposed Rule 213, OCC believes such changes will help to identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls, in accordance with Rule 17ad-22(e)(17)(i).³⁸

Consistency with Rule 17ad-22(e)(17)(ii)

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.³⁹ In addition to OCC's existing process that requires a Reconnection Attestation and Checklist to be submitted by a Clearing Member that has been disconnected, OCC's proposed changes to Rule 213 add provisions to strengthen the overall process and requirements around Reconnection of a Clearing Member. These changes include, but are not limited to: (i) the requirement that the subject Clearing Member submit the Reconnection Attestation prior to OCC reestablishing connectivity; (ii) the obligation for the subject Clearing Member to complete specific testing requirements prior to Reconnection in order to demonstrate to OCC that it is operationally ready to reconnect; and (iii) OCC's ability to request a report from a Third-Party Cybersecurity Firm, either as a condition to Reconnection or following Reconnection. By requiring that the subject Clearing Member (i)

³⁸ Id.

³⁹ 17 CFR 240.17ad-22(e)(17)(ii).

submit the Reconnection Attestation prior to OCC reestablishing connectivity, and (ii) complete specific testing requirements prior to OCC reestablishing connectivity, OCC will be able to better identify and address potential vulnerabilities that may still exist within the Clearing Member's environment after a Clearing Member System Event has occurred, and take steps to promote resiliency prior to establishing Reconnection. Furthermore, by including the ability for OCC to require an audit report from a Third-Party Cybersecurity Firm, OCC will be provided with key details about the Clearing Member System Event from a reputable and experienced source. OCC will be able to rely upon the information in the report to help analyze and address the Clearing Member System Event in effort to further mitigate risk. This, in turn, helps to strengthen OCC's security protocols. OCC believes these proposed changes provide OCC with the necessary tools to address and manage OCC's operational risks by ensuring, in part, that systems have a high degree of security, resiliency, and operational reliability, in accordance with Rule 17ad-22(e)(17)(ii).⁴⁰

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

Section 17A(b)(3)(I) of the Act⁴¹ 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 Rule 213 in effort to strengthen OCC's security protocols and promote resiliency when confronted with cybersecurity risks presented by OCC's interconnections with its Clearing Members. OCC believes the three of the proposed changes could have an impact on

⁴⁰ Id.

⁴¹ 15 U.S.C. 78q-1(b)(3)(I).

competition, but such impact is necessary and appropriate in further of the purposes of the Act.

The three proposed changes that OCC believes could have an impact on competition include: (i) adding the definition of a Third-Party Service Provider in proposed Rule 213(a)(6) to include an affiliate of any Clearing Member, service bureau or similar entity that connects to OCC's Systems on behalf of or for the benefit of a Clearing Member; (ii) adopting proposed Rule 213(g)(3), which provides OCC with the ability to require an audit report from a Third-Party Cybersecurity Firm; and (iii) establishing the requirements for testing prior to reconnection of a Clearing Member, as described in proposed Rule 213(h). As described below, although the three proposed changes may have an impact on competition, OCC believes that such impact is necessary and appropriate in further of the purposes of the Act.

Proposed Rule 213(a) establishes the definition of "Third-Party Service Provider" to include an affiliate of any Clearing Member, service bureau or similar entity, that connects to OCC's Systems on behalf of or for the benefit of a Clearing Member. Establishing the definition of Third-Party Service Provider for purposes of Rule 213 to include such entities described above could impose a burden on competition because such entities would now be explicitly subject to the requirements in Rule 213, including disconnection and Reconnection requirements. OCC acknowledges that being disconnected from OCC's Systems may impact the entity's ability to perform certain functions, therefore putting the entity at a competitive disadvantage. However, OCC believes that the proposed change would not create a significant burden. Based on OCC's critical role as a SIFMU, OCC has the responsibility to promote financial stability and protect the broader marketplace. Due to the close relationship and interconnectivity that exists between a Third-Party Service Provider and the related Clearing Member, OCC believes that it is critical to address risks presented by the Third-Party Service Provider that connects to OCC's Systems on

behalf of or for the benefit of a Clearing Member. Although this proposed change may impose a burden on such entity, OCC does not believe this burden is significant, and as described in proposed Rule 213(f)(1)(C), OCC would, as appropriate and practical, seek to facilitate the continuation of services for an entity that is subject to a Clearing Member System Event. Therefore, OCC believes the burden on competition is necessary and appropriate in furtherance of the purposes of the Act.

Proposed Rule 213(g)(3) provides OCC with the ability to require that the Clearing Member must provide an audit report from a Third-Party Cybersecurity Firm, either as a condition to Reconnection or following a Reconnection. Although this requirement may impose a burden on competition, OCC does not believe this burden is significant. As described above, given OCC's role as a SIFMU and its position in the marketplace, OCC believes it is prudent to enhance its management of Clearing Member System Events. OCC believes the ability to require, in certain circumstances, that the Clearing Member provide an audit report from a Third-Party Cybersecurity Firm will provide OCC with key details about the Clearing Member System Event. OCC believes this will help OCC analyze such incident and take necessary steps to mitigate risks presented. Although the Clearing Member may incur additional costs through the requirement to provide such audit report from a Third-Party Cybersecurity Firm, OCC believes this proposed change would not present an undue burden. OCC would also expect Clearing Members to leverage their existing relationships with Third-Party Cybersecurity Firms in effort to reduce costs of providing such audit report. OCC believes the proposed change is necessary to promote resiliency and enhance OCC's security protocols to protect OCC and Clearing Members from cybersecurity risks. Therefore, OCC believes the burden on competition presented by the proposed change is necessary and appropriate in furtherance of the Act.

OCC believes proposed Rule 213(h), which establishes testing requirements for Clearing Members prior to reconnection, may impose a burden on competition on a Clearing Member because the changes create additional steps that the Clearing Member must complete prior to reconnection. OCC acknowledges that these additional steps, if not completed by the Clearing Member, could result in a Clearing Member being disconnected from OCC's System's for a longer period of time than the Clearing Member would have expected, which may impose a burden on the Clearing Member. However, OCC believes that the burden on competition from the proposed testing requirements is necessary to help ensure that Reconnection is safe and appropriate. The purpose of the proposed testing requirements is to strengthen OCC's security protocols so that OCC can identify any vulnerabilities related to a Clearing Member System Event prior to establishing any Reconnection. Although this proposed change may impose a burden on the Clearing Member, OCC does not believe this burden is significant. In addition, proposed Rule 213(f)(1)(C), also provides that OCC will, as appropriate and practical, seek to facilitate the continuation of services of a disconnected Clearing Member, prior to Reconnection. Therefore, OCC believes the proposed change requiring testing requirements prior to Reconnection of a Clearing Member is necessary to help mitigate risk presented and ultimately protect OCC and other Clearing Members.

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.

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 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. Advance Notice Based on Rule of Another Self-Regulatory Organization or of the Commission

Not applicable.

Item 9. Security-Based Swap Submissions Filed Pursuant to Section 3C of the Exchange 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 Advance Notice for publication in the Federal Register.

Exhibit 3. OCC's Information Security Disconnection and Reconnection Procedure. [Confidential].

Exhibit 5. Proposed changes to OCC Rule 213.

EXHIBIT 1A

SECURITIES AND EXCHANGE COMMISSION

(Release No. 34-[]; File No. SR-OCC- 2026-010)

October __, 2026

Self-Regulatory Organizations; The Options Clearing Corporation; Notice of Filing of Proposed Rule Change by The Options Clearing Corporation concerning revisions to OCC Rule 213 – 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 October 8, 2026, 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

This proposed rule change would amend OCC Rule 213 – Cybersecurity Obligations (“Rule 213”) to further enhance OCC’s security protocols and promote resiliency in OCC’s approach to assessing and managing cybersecurity risks. OCC’s proposed changes to Rule 213 would, among other things, (i) establish the concept of a “Major Clearing Member System Event,” in which OCC would be authorized to take certain action, including disconnection of a Clearing Member, or its Third-Party Service

¹ 15 U.S.C. 78s(b)(1).

² 17 CFR 240.19b-4.

Provider, connected to OCC's Systems (as defined below); (ii) enhance the requirements of a Clearing Member to notify OCC in the event of a Security Incident (which would be redefined as a "Clearing Member System Event"); (iii) remove language that invites a Clearing Member to assess potential impact of a Clearing Member System Event on OCC's Systems and clarify OCC's authority to assess such incident and determine impact; (iv) provide OCC with the authority to inform, or require the Clearing Member to inform, the Clearing Member's Third-Party Service Provider (as defined below) of the Clearing Member System Event; (v) update and add defined terms used throughout Rule 213; and (vi) incorporate other reporting, testing and approval requirements, process, obligations, and governance necessary for reconnection.

The proposed changes to OCC Rule 213 are contained in Exhibit 5 to File No. SR-OCC-2026-010. Material proposed to be added is marked by underlining and material proposed to be deleted is marked with strikethrough text. All terms with initial capitalization that are not otherwise 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

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>.

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

Background

OCC is the sole clearing agency for standardized equity options listed on national securities exchanges registered with the Commission. OCC provides clearing services for options on equities, indices, Exchange Traded Funds ("ETFs"), for certain transactions in futures and options on futures, and for certain stock loan transactions. Organizations become OCC Clearing Members to facilitate the clearing and settlement of their customer transactions or proprietary transactions through OCC. More specifically, in its role as a clearing agency, OCC guarantees the performance of its Clearing Members for all transactions cleared by OCC by becoming the buyer to every seller and the seller to every buyer (or the lender to every borrower and the borrower to every lender, in the case of stock loan transactions). In 2012, OCC was designated as a systemically important financial market utility ("SIFMU") by the Financial Stability Oversight Council pursuant to Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 ("Dodd-Frank Act")⁴. Such designation highlights the critical role that OCC plays in ensuring the stability and integrity of the financial markets.

Based on OCC's interconnections with its Clearing Members and with its Clearing Member's Third-Party Service Provider connected to OCC's Systems, OCC is

⁴ Financial Stability Oversight Council 2012 Annual Report, Appendix A: Designation of Systemically Important Financial Market Utilities, at 145 (2012), <https://home.treasury.gov/system/files/261/2012-Appendix-A-Designation-of-Systemically-Important-Market-Utilities.pdf>.

exposed to various cybersecurity risks. Such cybersecurity risks have the potential to impact OCC, as well as market participants, as a cybersecurity attack on OCC may 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 SIFMU, a failure or disruption to OCC could threaten the stability of the financial system in the United States. Therefore, OCC believes it is prudent to enhance the cybersecurity notification obligations of its Clearing Members and strengthen OCC's ability to protect against and respond to such events to safeguard OCC's Systems and information against cyberattacks.

In November 2023, OCC received approval⁵ from the Commission to amend certain provisions in OCC's Rules relating to a Clearing Member's obligation to address a "Security Incident" (currently defined as 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). The amended provisions became OCC's existing Rule 213, which established, among other things: (i) notification requirements of a Clearing Member in the event of a Security Incident and (ii) OCC's security requirements for the reconnection process of a Clearing Member following a Security Incident that results in a Clearing Member's disconnection.

In recent years, OCC has received Rule 213 notifications, however, none have impacted OCC. OCC monitors the threat landscape on an ongoing basis, maintaining a dedicated threat intelligence team responsible for monitoring the activities of threat actors

⁵ See Securities Exchange Act Release No. 98979 (Nov. 17, 2023), 88 FR 82441 (Nov. 24, 2023) (SR-OCC-2023-003).

targeting the financial services industry. Through this monitoring, OCC has observed an increase in the frequency and elevated risk of cyber events targeting the industry and the broader marketplace. Considering OCC's experience receiving Rule 213 notifications, together with the increasing frequency and elevated risk of cyber events in the financial services industry at large, OCC has identified opportunities for additional enhancements to Rule 213. Though no specific triggering event necessitated these enhancements, OCC's actions are proactive, taken in light of the elevated risk environment across the industry.

1. Purpose

OCC's proposed amendments to Rule 213 are intended to further promote resiliency, strengthen OCC's cybersecurity protocols, and maintain consistency with industry standards, including by aligning OCC's Rules with recent rule amendments⁶ of similarly situated self-regulatory organizations ("SROs") with overlapping membership with OCC. Among other things, OCC's proposed enhancements to Rule 213 would:

- Add a defined terms section to Rule 213, including defining OCC's "Systems" to include not only direct connections, but also established communication channels (e.g., access to File Transfer Protocols ("FTPs") for transmitting data or instructions that may be compromised by a systems intrusion to a Clearing Member's back-office systems);

⁶ See Securities Exchange Act Release No.104183 (Nov. 17, 2025), 90 FR 52453 (Nov. 20, 2025) (SR-DTC-2025-003), (SR-FICC-2025-006), (SR-NSCC-2025-003).

- Require the Cybersecurity Confirmation to be signed by a senior executive of the Clearing Member or applicant who is authorized to attest to such matters;
- Remove language that invites a Clearing Member to assess the potential impact of a Clearing Member System Event on OCC's Systems and operations when determining whether such incident is reportable, specify the timeframe in which OCC requires a Clearing Member System Event to be reported, and identify the specific information a Clearing Member must include in such notice;
- Establish the concept of a "Major Clearing Member System Event," including a declaration requiring the approval of two or more Designated Officers and prompt notification to the Chairman of the Board of Directors;
- Reorganize and clarify OCC's authority to take action in response to a Clearing Member System Event, including specifying the actions that constitute a "disconnect," and clarify a Clearing Member's related cooperation obligations;
- Add provisions incorporating the reporting, testing, and approval requirements, process, obligations, and governance necessary for reconnection, including the ability for OCC to require an audit report from a Third-Party Cybersecurity Firm; and
- Provide OCC with the authority to inform, or require the Clearing Member to inform, the Clearing Member's Third-Party Service Provider of the

Clearing Member System Event if OCC determines, in its discretion, that such action is necessary for the protection of OCC and other Clearing Members.

As described in more detail below, OCC believes its proposed changes will strengthen OCC's security protocols by enhancing Rule 213 to be more efficient, effective and clear in its cybersecurity obligations of Clearing Members so that OCC may better address cybersecurity risks to protect OCC and its Clearing Members. Furthermore, OCC believes its proposed changes will enable OCC's Clearing Members to better understand and prepare for their obligations to OCC as it relates to a cybersecurity event.

Proposed Changes

Proposed Rule 213(a)⁷ – Defined Terms

First, OCC proposes to introduce new section (a) titled "Defined Terms." To strengthen the provisions of proposed Rule 213 and further clarify OCC's requirements related to the cybersecurity obligations of a Clearing Member, OCC proposes to define several terms specifically for the purposes of Rule 213.⁸ OCC's proposed changes would:

- Define "Best Practices" to mean policies, procedures, practices or similar standards and guidelines that are reasonably designed and consistent with then current financial-sector cybersecurity standards issued by an authoritative body that is a U.S. governmental entity or agency, an association of a U.S.

⁷ Existing Rule 213(a) would be renumbered to Rule 213(b).

⁸ OCC's proposed amendments to Rule 213 align with the rule amendments of similarly situated SROs with overlapping membership with OCC, including the National Securities Clearing Corporation ("NSCC"). See supra note 6.

governmental entity or agency, or a widely recognized industry organization.

The purpose of defining “Best Practices” is to clarify the standards that OCC would require a Third-Party Cybersecurity Firm to employ when such firm is engaged, as would be required by OCC Rule 213 as discussed further below.

OCC’s proposed definition of “Best Practices” aligns with Section 1001(a)(4) of the Commission’s Regulation Systems Compliance and Integrity (“Reg SCI”).⁹

- Delete OCC’s existing definition of a “Security Incident” and replace it with “Clearing Member System Event.” OCC proposes to define a “Clearing Member System Event” to mean an incident resulting from the unintended or unauthorized access to, or the malfunction or corruption (whether partial or total) of one or more systems, of a Clearing Member or its Third-Party Service Provider, connected to OCC’s Systems. The purpose of re-defining the concept of a “Security Incident” to a “Clearing Member System Event” is to capture only those disruptions to systems connected to OCC’s Systems, whether via an established communication channel from a Clearing Member, or through the Clearing Member’s Third-Party Service Provider; it is not intended to capture every disruption to every system of the Clearing Member or its Third-Party Service Provider. In addition, as described in further detail in section (d) of proposed Rule 213, OCC proposes to eliminate the existing definition of a “Security Incident” to remove language that invites Clearing Members to assess the potential impact of such incident on OCC’s Systems

⁹

17 CFR 242.1001(a)(4).

and operations when determining whether an incident is reportable. OCC's existing definition of a "Security Incident," is defined, in part, as an incident, or an incident that is occurring, involving a cyber-related disruption or intrusion of the Clearing Member's systems that is reasonably likely to pose an imminent risk or threat to OCC's operations. OCC believes the language in the existing definition invites Clearing Members to assess whether such incident to their systems would impact OCC, and therefore OCC proposes to eliminate the definition of "Security Incident" and replace the definition with "Clearing Member System Event" in proposed Rule 213.

- Define "OCC's Systems" to mean the systems, equipment and technology networks of OCC, whether owned, leased, or licensed, and including software, hardware, applications, devices, IP addresses, or other addresses or accounts used in an established communication channel with such systems, equipment and technology networks, to provide the services set forth in these Rules, or otherwise used to transact business or connect with OCC. OCC proposes to introduce the definition of "OCC's Systems" for the purposes of Rule 213 to articulate OCC's potentially impacted connections and any means of connectivity in the event of a Clearing Member System Event. OCC's proposed definition incorporates not only direct connections but also references "established communication channels," which OCC believes may include access to File Transfer Protocol ("FTP's") for transmitting data or instructions that may be compromised by a systems intrusion to a Clearing Member's back-office systems.

- Define a “Major Clearing Member System Event” to mean a Clearing Member System Event that has or is reasonably anticipated to, for example, disrupt, degrade, cause a delay in, interrupt or otherwise alter the normal operation of OCC’s Systems; result in unauthorized access to OCC’s Systems; result in the loss of control of, disclosure of, or loss of OCC’s Confidential Information; or cause a strain on, loss of, or overall threat to the OCC’s resources, functions, security or operations. The purpose of establishing the concept of a “Major Clearing Member System Event,” is to tie the disruption at issue to its effect on the normal operations of OCC. This concept introduces a threshold level in which OCC would be authorized to take action, including disconnection, in the event OCC determines that a Clearing Member System Event rises to the level of a Major Clearing Member System Event.¹⁰ OCC believes the concept of a “Major Clearing Member System Event” will strengthen OCC’s security protocols by establishing a baseline by which OCC can measure the disruption at issue against its impact on OCC and, as described in further detail below, take action to mitigate risks presented.
- Define “Third-Party Cybersecurity Firm” to mean a firm that, in OCC’s reasonable judgement, (A) (i) is well-known and reputable; (ii) is not the subject Clearing Member, or an affiliate or a Third-Party Service Provider of the subject Clearing Member; (iii) is experienced in financial-sector cybersecurity; and (iv) employs Best Practices; or (B) is otherwise determined

¹⁰

OCC’s Information Security Disconnect and Reconnect Procedure is contained in Confidential Exhibit 3 of SR-OCC-2026-010, and it outlines how OCC determines that a Clearing Member System Event rises to the level of a Major Clearing Member System Event.

to be a Third-Party Cybersecurity Firm by OCC. OCC proposes to include this definition to clearly describe the type of firm that OCC would require the subject Clearing Member to engage under proposed Rule 213(g)(3).

- Define “Third-Party Service Provider” to mean an affiliate of any Clearing Member, service bureau or other similar entity, that connects to OCC’s Systems on behalf of or for the benefit of a Clearing Member. This proposed definition would help clarify that OCC Rule 213 applies to a Clearing Member’s Third-Party Service Provider’s connections to OCC’s Systems.

Proposed Rule 213(b) – Cybersecurity Confirmation Submission

Proposed Rule 213(b) incorporates the provision from existing Rule 213(a)(ii) into proposed Rule 213(b)(1) to promote clarification and efficiency. Proposed Rule 213(b) also makes other conforming and non-substantive changes, including reorganizing provisions into a hierarchical structure, and updating language to promote clarity and efficiency.

Existing Rule 213(a) requires Clearing Members and clearing membership applicants to periodically submit a form, provided by OCC, confirming, in part, that they have a cybersecurity program in place (“Cybersecurity Confirmation”). Sections (i) and (ii) of existing Rule 213(a) require that applicants must submit it with their application, and existing Clearing Members must resubmit it at least every two years, within 180 days of the OCC’s notice requiring attestation. OCC’s proposed changes streamline existing Rule 213(a) into proposed Rule 213(b)(1) by combining the general description of the Cybersecurity Confirmation requirement with the specific timing obligation applicable to Clearing Members into a single paragraph. Specifically, OCC’s proposed Rule 213(b)(1) would provide, in part, that each Clearing Member must complete and submit “an

attestation at least every two years, and not later than 180 calendar days from the date that OCC notifies the Clearing Member that the attestation is required.” In addition, proposed Rule 213(b)(1) would remove the reference to the phrase “applicant for clearing membership” as OCC believes such language is duplicative since it is included in the subsequent provision in proposed Rule 213(b)(2). OCC’s proposed changes replace the term “shall” with “must” in proposed Rule 213(b)(1) and proposed Rule 213(b)(2) to promote stronger cadence and readability. OCC’s proposed changes also eliminate the specific reference to the word “form” after “attestation.” The concept of a “form” and an “attestation” may introduce different meanings, so this proposed change is intended to eliminate ambiguity and maintain consistency with OCC’s referenced term, “Cybersecurity Confirmation.” OCC also proposes to eliminate the reference that the attestation is “provided by the Corporation” because OCC believes this is unnecessary to specify. Finally, OCC proposes to remove the word “materials” in proposed Rule 213(b)(2) to promote efficiency.

Proposed Rule 213(c)¹¹ – Representations in the Cybersecurity Confirmation

OCC’s proposed changes relocate the signature requirement set forth in existing Rule 213(c), “Execution of the Cybersecurity Confirmation,” into the introductory provision of proposed Rule 213(c), “Representations in the Cybersecurity Confirmation” (redesignated from existing Rule 213(b)). As relocated, the requirement would provide that the Cybersecurity Confirmation must be signed by a senior executive of the Clearing Member or applicant who is authorized to attest to these matters, consistent with the substance of the existing requirement. Existing Rule 213(c) would be deleted in its

¹¹ Existing Rule 213(b) would be renumbered to proposed Rule 213(c).

entirety, as its sole requirement is preserved within proposed Rule 213(c). OCC believes this change is non-substantive and is designed to eliminate duplicative rule text and improve the clarity and organization of Rule 213. OCC's proposed changes also remove the word "designated" from the signature requirement, such that the Cybersecurity Confirmation may be signed by any senior executive of the Clearing Member or applicant who is authorized to attest to these matters, rather than requiring a designated senior executive. Specifically, proposed Rule 213(c) would provide that the Cybersecurity Confirmation "must be signed by a senior executive of the Clearing Member or applicant who is authorized to attest to these matters." OCC believes the term "designated" creates ambiguity. Additionally, OCC believes that removing this term improves operational flexibility by allowing any senior executive with the requisite authorization to sign and improves timely compliance by avoiding delays that could arise if a specifically designated individual is unavailable at the time attestation is required. OCC believes the proposed change preserves the integrity and reliability of the attestation, since the signatory must still be a senior executive with the requisite authorization to attest to these matters.

OCC's proposed changes to Rule 213(c) also make other non-substantive changes, including reorganizing the provisions into a hierarchical structure and replacing the term "shall" with "must" to promote stronger cadence and readability.

Proposed Rule 213(d) – Occurrence of a Clearing Member System Event

OCC's proposed Rule 213(d) would introduce enhanced notification requirements for a Clearing Member in the event of a Clearing Member System Event. More specifically, OCC's proposed changes would introduce a particular timeframe required

for Clearing Members to report such incident and specify the information that must be included in the notification.

First, as referenced above in the proposed “Defined Terms” section, OCC proposes to re-define and broaden the definition of “Security Incident” to “Clearing Member System Event.” In alignment with this proposed change, OCC would also eliminate the existing definition of a “Security Incident” in proposed Rule 213(d), which states in part, that such incident is one that is occurring involving a cyber related disruption or intrusion of the Clearing Member’s systems that is reasonably likely to pose an imminent risk or threat to OCC’s operations.

Second, OCC’s proposed changes would require that a Clearing Member experiencing a Clearing Member System Event must notify OCC immediately “in writing, but no later than two hours” after the Clearing Member becomes aware or should be aware that there has been a Clearing Member System Event. The purpose of including a specific timeframe of two hours for which a Clearing Member System Event must be reported is to clarify OCC’s existing standard of “immediate” in order to help mitigate the risk presented by a Clearing Member or its Third-Party Service Provider that is experiencing such incident.¹² OCC believes that the term “immediately,” standing alone, may be interpreted differently and therefore could create uncertainty and inconsistent compliance. By pairing “immediately” with a definite, objective two-hour limit, OCC’s Clearing Members will have a clear, unambiguous benchmark for timely notification. By receiving notification of a Clearing Member System Event within two hours of its

¹² OCC’s current rule 213(d) requires a member to immediately notify OCC and to confirm such notice promptly in writing.

occurrence, OCC believes it will be able to address and respond to such event in a timely manner and take proactive steps to reduce any future risk presented to OCC and its Clearing Members. If a Clearing Member does not report a Clearing Member System Event within the notification timeframe set forth in section (d), OCC will evaluate the facts and circumstances of the delay in notification to determine whether a rule violation has occurred that is subject to OCC's disciplinary process under Chapter XII of OCC's Rules.

Third, OCC's proposed changes require that notification of proposed section 213(d) must, at a minimum include the following information (as described below), and any such information unconfirmed or otherwise unknown may be identified by the Clearing Member as "Unknown." OCC's existing Rule 213 does not expressly set out requirements for what to include in a notification of a Clearing Member System Event. While OCC already obtains the required information outlined out in proposed Rule 213(d) through its existing practice, the required information is not memorialized in OCC's Rules, policies, or procedures. This practice has historically included, among other things, requests regarding the legal entity name of the Clearing Member, contact information of individuals authorized to act on its behalf, and key details of the incident such as its nature, status, systems or data affected, and remediation steps taken. OCC typically obtains this information from the Clearing Member via phone or email, depending on the circumstances. This information is generally gathered over the course of OCC's engagement with the Clearing Member as the incident develops and the Clearing Member's own understanding of the incident evolves, rather than all at once at the onset of the incident. As such, the purpose of proposed section 213(d) is to codify

what OCC already expects in practice, so that all Clearing Members are aware, in advance, of the information required to be included when reporting a Rule 213 incident.

OCC's proposed changes provide that the information required to be in the notice, if known, include: (i) the legal entity name of the Clearing Member or its Third-Party Service Provider affected by the Clearing Member System Event, (ii) contact information of individuals who are authorized to act on behalf of the subject Clearing Member regarding the Clearing Member System Event, and (iii) key details of the Clearing Member System Event such as event type, event effect, start date, end date, discovery date, scope, and any other notices given that would help to provide additional context of the Clearing Member System Event. As discussed above, OCC's existing Rule 213 does not expressly set out requirements for what information must be included in a notification of a Clearing Member System Event. In practice, OCC would obtain the same details identified in proposed section 213(d), but not all at once and not in the formal manner that proposed section 213(d) establishes.

OCC's proposed changes to Rule 213(d) would provide that the information required in the notice related to "Legal Entities" would include a complete list of the legal entity names of the Clearing Member and any Third-Party Service Providers experiencing or otherwise affected or potentially affected by the Clearing Member System Event. In addition, OCC's proposed changes would require that information required in the notice related to "Contact Information" would include list of persons – with their corresponding titles, primary email addresses and phone numbers, and if those primary email addresses and phone numbers are associated with the systems that are the subject of the Clearing Member System Event, alternate email addresses and phone

numbers – who are authorized to act on behalf of the subject Clearing Member regarding the Clearing Member System Event. Furthermore, OCC’s proposed changes would provide that information required in the notice related to “Clearing Member System Event Details” would include requirements in sections (A) through (G) of proposed Rule 213(d):

(A) Event Type – the type of Clearing Member System Event, for example an insider threat, phishing attack, Man-in-the-Middle (“MITM”)¹³ attack, privilege escalation, denial of service, external threat, malware, unauthorized access, ransomware, compromised user account, SQL injections, brute force attack, system compromise, supply chain attacks (as each term is commonly understood by cybersecurity professionals in the financial sector), or other with a provided explanation;

(B) Event Effect – perceived, anticipated, or known effect of the Clearing Member System Event, for example, loss of communication, data corruption, security breach, or other with a provided explanation;

(C) Start Date – date and time when the Clearing Member System Event began;

(D) End Date – date and time when the Clearing Member System Event ended, if applicable;

(E) Discovery Date – date and time when the Clearing Member System Event was first identified;

(F) Scope – scope of the Clearing Member System Event, including, but not

¹³ A man-in-the-middle (“MITM”) attack is an attack in which an adversary positions itself between two communicating parties in order to intercept and alter the data traveling between them. See National Institute of Standards and Technology, Computer Security Resource Center, Glossary, Man-in-the-Middle Attack (MitM), https://csrc.nist.gov/glossary/term/man_in_the_middle_attack.

limited to, a list of each affected or likely affected system or data, including OCC's Systems and data, the degree of such affect, and any supporting evidence of such; and

(G) Notices – whether any formal or informal notices or information regarding the Clearing Member System Event was made public and, if so, provide a copy of such notices or information.

The purpose of these proposed changes is to codify OCC's expectations to increase transparency around OCC's existing process. More specifically, OCC's proposed changes codify, within Rule 213(d), the information that OCC has historically requested from Clearing Members during a Rule 213 event. Currently, OCC receives this information from Clearing Members upon request during a Rule 213 event as an incident unfolds, rather than receiving a standardized set of information upfront. By codifying OCC's expectations directly in this Rule, OCC intends to increase transparency and ensure that all Clearing Members know, in advance, precisely what information they must provide when reporting a Rule 213 incident, as well as the types of information OCC may request as its investigation proceeds. OCC believes this advance clarity will enable Clearing Members to prepare more effectively and will allow OCC to more promptly and effectively review and mitigate any risk associated with the incident.

OCC believes that the requested information in the proposed sections (A) through (G), including Legal Entities, Contact Information, and details of the Clearing Member System Event are essential pieces of information that would help OCC to efficiently and effectively review and take action to mitigate risk presented. OCC also believes the proposed changes will allow Clearing Members and their Third-Party Service Providers to better understand and prepare for their obligations to OCC in the event they experience

a Clearing Member System Event.

Proposed Rule 213(e)¹⁴ – Declaration of a Major Clearing Member System

Event

OCC proposes to introduce new Rule 213(e) sections (1) through (3), which would focus on the declaration of a Major Clearing Member System Event, including the details surrounding who is authorized to declare such event and notification requirements associated with such event.

First, proposed Rule 213(e)(1) would provide that upon becoming aware of a Clearing Member System Event, OCC will consider whether such Clearing Member System Event meets the definition of a Major Clearing Member System Event. The proposed change would also provide that the existence of a Major Clearing Member System Event must be declared by two or more Designated Officers of OCC, in their reasonable judgement.

Second, proposed Rule 213(e)(2) would provide that upon declaration of a Major Clearing Member System Event, OCC may act (or refrain from acting) pursuant to this Rule to help address, correct, mitigate or alleviate any and all risks presented to OCC by or related to the Major Clearing Member System Event. The proposed change would also provide that action taken will be in consideration of the risks presented to OCC, including but not limited to, information provided pursuant to this Rule.

The purpose of OCC's Proposed Rule 213(e)(1) through (2) is to clarify that OCC will assess the potential impact of a Clearing Member System Event on OCC's Systems and operations, and OCC will determine to act, or refrain from acting, depending on the

¹⁴ Existing Rule 213(e) would be renumbered to Rule 213(g).

details of the Clearing Member System Event. The proposed rule removes any ambiguity that may exist in present language that invites the Clearing Member to assess potential impact of the Clearing Member System Event on OCC's Systems or operations. The purpose of the proposed change is also to clearly define who is authorized to declare a Major Clearing Member System event, specifically, that such a declaration must be made by two or more Designated Officers of OCC. OCC believes it is appropriate that such declaration be made by two or more Designated Officers of OCC to ensure that information regarding the Clearing Member System Event has been escalated to and considered at the highest management level. OCC believes the proposed rule change also provides transparency to Clearing Members and other stakeholders as to who is authorized to declare a Major Clearing Member System Event.

Lastly, OCC's proposed changes introduce a new requirement that OCC notify the Chairman of the Board of Directors following a declaration of a Major Clearing Member System Event. Specifically, proposed Rule 213(e)(3) provides that following declaration of a Major Clearing Member System Event, OCC will promptly notify the Chairman of the Board of Directors of such declaration. Because a Major Clearing Member System Event reflects OCC's determination that a Clearing Member System Event may have a significant impact on OCC's Systems or operations, OCC believes it is appropriate that this information be escalated to the Chairman of the Board of Directors without delay. OCC believes that notifying the Chairman is appropriate because it allows the Chairman to determine, based on the nature and severity of the specific Major Clearing Member System Event, the extent to which the full Board or any relevant Board Committee should be further notified or involved.

Proposed Rule 213(f) – Authority to Take Action and Required Cooperation

Proposed Rule 213(f) would expand upon OCC’s existing authority to take action in the event of a Clearing Member System Event and associated Major Clearing Member System Event. More specifically, proposed Rule 213(f) introduces requirements surrounding: (i) OCC’s ability to act, or refrain from acting, in the event of a Major Clearing Member System Event, (ii) OCC’s responsibility to notify the Clearing Member of any disconnect or material action taken, and (iii) the Clearing Member’s responsibility to cooperate fully and to the reasonable satisfaction of OCC in the event of a Major Clearing Member System Event. Proposed Rule 213(f) also makes other conforming and non-substantive changes, including reorganizing provisions into a hierarchical structure, and updating language to promote clarity and efficiency.

OCC’s proposed changes would organize Rule 213(f) into subsections (1) through (4). Proposed Rule 213(f)(1) details, in part, OCC’s ability to, in the event of a Clearing Member System Event, take actions reasonably necessary to mitigate any impact to its operations, including actions described in proposed Rule 213(f)(1)(A) through Rule 213(f)(1)(C).¹⁵ OCC’s changes to proposed Rule 213(f)(1)(A) make conforming and non-substantive changes to the text, including removing the phrase “the right to.” To maintain consistency and align with OCC’s proposed definition of OCC’s Systems, OCC proposes to eliminate the term “data” before systems in proposed Rule 213(f)(1)(A). Proposed Rule 213(f)(1)(B) is new and provides that OCC may take actions reasonably necessary to mitigate any effects to its operations, including to suspend any and all transmissions,

¹⁵ The proposed changes would not substantively alter this section of 213(f) but include only conforming changes such as changes to match defined terms.

communications, or access between OCC's Systems (together with actions taken under Rule 213(f)(1)(A), "disconnect"). The purpose of this change is to broaden OCC's authority to take action that OCC believes may be necessary to mitigate risk presented by a Clearing Member System Event and associated Major Clearing Member System Event. In addition to OCC's existing authority to disconnect access of a Clearing Member, as described in proposed Rule 213(f)(1)(A), OCC believes the proposed change to expand OCC's authority to suspend any and all transmission, communication or access of a Clearing Member will help to ensure that OCC can adequately address all potential connectivity and communication types of a Clearing Member. OCC also proposes to adopt new Rule 213(f)(1)(C) to provide OCC the authority to act in the event OCC determines that a Major Clearing Member System Event has occurred. Proposed Rule 213(f)(1)(C) provides that OCC may take, or refrain from taking, or require the subject Clearing Member to take or refrain from taking, any and all action that OCC considers appropriate to help address, correct, mitigate or alleviate the Major Clearing Member System Event and, as appropriate and practical, facilitate the continuation of services, which may include issuing instructions to the subject Clearing Member and requiring such Clearing Member to act on such instructions. Examples of actions that OCC considers appropriate may include, but are not limited to, disconnection from OCC's Systems, forced password resets, and requiring the Clearing Member to use alternative communication and file transfer methods (e.g. secure file transport instead of email). The purpose of this proposed change is to provide OCC with the authority to evaluate and address a Major Clearing Member System Event and adequately respond to such event in effort to mitigate impact to OCC and its Clearing Members. Additionally, in the event

OCC determines a Major Clearing Member System Event has occurred, by adding the provision that allows OCC to issue instructions and requires the subject Clearing Member to follow those instructions, OCC believes this requirement will help to help facilitate the continuation of services for the subject Clearing Member and alleviate future impact that may otherwise result from the disruption. Specifically, the issuance of instructions allows OCC to direct a more tailored response that is specific to the nature and severity of the Major Clearing Member System Event. This flexibility enables OCC to address the risk presented by a specific Major Clearing Member System Event while, where practicable, preserving the Clearing Member's ability to continue some or all of its services during remediation.

OCC proposes to adopt Rule 213(f)(3), which addresses OCC's notification requirements to the Clearing Member, as well as the subject Clearing Member's obligations to comply with OCC's statutory rules. More specifically, proposed Rule 213(f)(3) would provide that OCC will promptly notify the Clearing Member of any disconnect or other material action that OCC takes with respect to such Clearing Member pursuant to Rule 213. In addition, proposed Rule 213(f)(3) would provide that, notwithstanding any action taken pursuant to Rule 213, the Clearing Member must continue to meet its obligations to OCC and comply with OCC's statutory rules, as defined in its By-Laws. Under OCC's existing Rule 213, if OCC determines that disconnection of a Clearing Member from OCC's Systems is necessary, the Clearing Member must continue to meet its obligations to OCC notwithstanding that disconnection. OCC's existing Rule 213(d) focuses solely on the Clearing Member's continuing obligations following a disconnection and it does not address whether OCC

will notify the Clearing Member that a disconnection (or any other action) has occurred.

Proposed Rule 213(f)(3) expands the current provision in two respects: (i) it adds a notification obligation on OCC's part, and (ii) it broadens both the scope of triggering actions (from disconnection alone to any material action under the Rule) and the scope of the Clearing Member's continuing obligations to also include compliance with OCC's statutory rules, as the term is defined in OCC's By-Laws.

These proposed changes serve several purposes. First, the purpose of requiring OCC to promptly notify a Clearing Member of any disconnection or other material action taken under this Rule is to provide enhanced transparency to Clearing Members regarding actions that OCC takes that impact them. OCC believes it is prudent to notify the Clearing Member promptly in such event to allow the Clearing Member to better prepare for and understand their obligations to OCC. Second, the proposed change expands the scope of that notification obligation from disconnection alone to "any material action" taken pursuant to the Rule. This may include, for example, modifying the scope and specifications of access of the Clearing Member to OCC's Systems. The purpose of this proposed change is to ensure that Clearing Members receive notice of any material action OCC may take, not solely the most severe action of disconnection. Third, the proposed change broadens the Clearing Member's continuing obligations to apply "notwithstanding any action taken pursuant to this Rule," rather than only "notwithstanding disconnection," removing any ambiguity as to whether a Clearing Member's obligations to OCC continue in the event OCC takes a material action, outside of disconnection. Finally, the proposed change also specifies what obligations the Clearing Member must continue to meet, by adding an express requirement that the

Clearing Member comply with the statutory rules of OCC, as defined in OCC's By-Laws. OCC's current Rule 213 refers only generally to the Clearing Member's "obligations to OCC" without specifying what those obligations include. OCC believes the addition of "comply with the statutory rules of OCC, as defined in its By-Laws" clarifies what those obligations encompass. OCC's proposed changes to proposed Rule 213(f)(3) also make other conforming, non-substantive changes.

Lastly, OCC proposes to adopt new Rule 213(f)(4), which requires that the Clearing Member must cooperate fully and completely with, and to the reasonable satisfaction of, OCC in all matters relating to the Major Clearing Member System Event, including, but not limited: (i) conducting timely investigations and inquiries, as OCC believes reasonably necessary, with respect to any known or unknown information relating to the Clearing Member System Event; (ii) promptly notifying OCC of any material changes, updates, or new information learned regarding the Clearing Member System Event; and (iii) promptly providing any documentation or information requested by OCC, unless not legally permitted to do so, regarding or related to the Clearing Member System Event.¹⁶ The purpose of this proposed change is to provide enhanced transparency to Clearing Members on their obligations to comply with the proposed requirements. OCC believes that cooperation from Clearing Members on matters relating to a Major Clearing Member System Event will help OCC to efficiently and effectively manage and respond to a Major Clearing Member System Event in effort to mitigate risk presented.

¹⁶ Sections (i) through (ii) described in the narrative would be numbered to proposed Rule 213(f)(4)(A) though proposed Rule 213(f)(4)(C).

Proposed Rule 213(g)¹⁷ Procedures for Reconnection

OCC proposes to update existing Rule 213(e) titled “Procedures for Connecting Following a Security Incident that Results in Disconnection” to Proposed Rule 213(g) titled “Procedures for Reconnection.” OCC believes that such change in title is necessary to more accurately encompass the obligations of a Clearing Member pursuant to OCC’s authority to act in the event of a Clearing Member System Event, as described in proposed Rule 213(f)(1). The retitled rule sets forth the information that the subject Clearing Member would be required to provide OCC in the event OCC takes action pursuant to proposed Rule 213(f)(1) and includes both substantive and non-substantive changes as described below. Proposed Rule 213(g) also reorganizes existing Rule 213(e) into proposed Rule 213(g)(1) through 213(g)(2), and incorporates new section (3) in proposed Rule 213(g)(3) titled “Report from Third-Party Cybersecurity Firm.”

Proposed Rule 213(g)(1) Reconnection Attestation

OCC’s proposed Rule 213(g)(1) would be titled “Reconnection Attestation.” Proposed Rule 213(g)(1) would include the current requirement that a subject Clearing Member must complete and submit a Reconnection Attestation prior to OCC reestablishing connectivity to OCC’s Systems. More specifically, proposed Rule 213(g)(1) would provide that if OCC takes action pursuant to Rule 213(f)(1), the Clearing Member must complete and submit a form as provided by OCC that describes the Clearing Member System Event and includes required representations (“Reconnection Attestation”). OCC proposes to add language to clarify that such requirement must be met prior to OCC reestablishing connectivity to OCC’s Systems (“Reconnection”). OCC

¹⁷

Existing Rule 213(e) would be renumbered to proposed Rule 213(g).

proposes to relocate the existing provision that states “The Clearing Member also will be required to complete an associated checklist provided by OCC that describes remediation efforts (“Reconnection Checklist”),” because OCC believes such text is more appropriately located in proposed Rule 213(g)(2), which outlines the requirements in the Reconnection Checklist. In addition, OCC’s proposed changes collapse and consolidate Rule 213(e)(1) into Rule 213(e), which becomes proposed Rule 213(g), such that the signature requirement is now reflected in proposed Rule 213(g)(1). Specifically, OCC’s proposed changes reflect that the provision in current Rule 213(e)(1) on the requirement for the Reconnection Attestation to be signed by a designated senior executive becomes included in proposed Rule 213(g)(1). This change is intended to make Rule 213 easier to navigate by grouping related requirements together; it does not alter the Clearing Member’s underlying obligation to obtain a signature from an individual who maintains the authorization to sign the Reconnection Attestation. OCC’s proposed changes also eliminate the term “designated” when describing the senior executive of the Clearing Member that must sign the Reconnection Attestation. OCC believes the term “designated” creates ambiguity. By removing this term, OCC believes it improves operational flexibility by allowing any senior executive of the Clearing Member¹⁸ with the requisite authorization to sign, and it improves timely compliance by avoiding delays that could arise if a specifically designated individual is unavailable at the time attestation

¹⁸

A senior executive of the Clearing Member with the requisite authorization to sign may for example include, but is not limited to, a member of the board of directors or a member of senior management with the requisite knowledge and experience to make such an attestation, as determined by the Clearing Member’s own delegation of authority and procedures.

is required. OCC believes the proposed change preserves the integrity and reliability of the attestation, since the signatory must still be a senior executive with the requisite authorization to attest to these matters.

In addition, proposed Rule 213(g)(1)(A) through 213(g)(1)(E) incorporates the requirements in current Rule 213(e)(1)(A) through Rule 213(e)(1)(E) and makes other non-substantive changes including renaming the term “Security Incident” to “Clearing Member System Event,” as described in proposed Rule 213(a).

Proposed Rule 213(g)(2) Reconnection Checklist

OCC’s proposed Rule 213(g)(2) would be titled “Reconnection Checklist.” Proposed Rule 213(g)(2) reorganizes the provisions from existing Rule 213(e)(2) into proposed Rule 213(g)(2) and subsections (A) through (J) of proposed Rule 213(g)(2) to promote clarity and efficiency. OCC’s proposed changes also make other conforming, clarifying and non-substantive changes. More specifically, OCC’s proposed changes to Rule 213(g)(2) provide that if OCC takes action pursuant to Rule 213(f)(1), the Clearing Member must complete an associated checklist as provided by OCC that describes remediation efforts (“Reconnection Checklist”), which may require information including but not limited to the information in proposed subsections (A) through (J) of proposed Rule 213(g)(2).

Proposed Rule 213(g)(3) Report from Third-Party Cybersecurity Firm

OCC proposes to adopt Rule 213(g)(3), titled “Report from Third-Party Cybersecurity Firm,” which provides that OCC may require that the subject Clearing Member provide a report from a Third-Party Cybersecurity Firm, either as a condition to Reconnection or following Reconnection. OCC’s proposed changes describe the

information required to be in such report in proposed Rule 213(g)(3)(A) through proposed Rule 213(g)(3)(G).

More specifically, proposed Rule 213(g)(3) states that if OCC takes action pursuant to Rule 213(f)(1), OCC may require, either as a condition to reconnection or following reconnection, that the Clearing Member provide a detailed, comprehensive, and auditable report from a Third-Party Cybersecurity Firm, or a summary of such report that includes: (i) a timeline of the Clearing Member System Event, including all material actions, events, and decisions taken for or relating to the Clearing Member System Event; (ii) a description of the Clearing Member System Event and an explanation of how such disruption was corrected or resolved; (iii) root cause analysis of the Clearing Member System Event; (iv) confirmation that any issues identified by the Third-Party Cybersecurity Firm as severe, critical, or moderate, or comparable categorizations, have been resolved; (v) confirmation of normal or intended operation of the subject system(s), including, but not limited to, the return or replacement of key systems and data stores to pre-Clearing Member System Event resilience, in a safe, secure and proper manner for at least 72 hours; (vi) a description of short-and long-term preventive monitoring and detection recommendations from the Third-Party Cybersecurity Firm; and (vii) any other information reasonably requested to be included by OCC.¹⁹ In the event a Clearing Member is the subject of action pursuant to OCC's authority under proposed Rule 213(f)(1), the purpose of proposed Rule 213(g)(3) is to provide OCC with all necessary information about the subject Clearing Member's disruption and its remediation from an

¹⁹ The provisions described in subsections (i) through (vii) above would be organized as subsections (A) through (G), respectively, in proposed Rule 213(g)(3).

independent, knowledgeable and reputable Third-Party Cybersecurity Firm, so that OCC can determine whether Reconnection is appropriate. OCC's ability to require an audit report from a Third-Party Cybersecurity Firm provides OCC with essential information that will help OCC to fully evaluate the Clearing Member System Event and take steps to mitigate risks presented by such incident.

Proposed Rule 213(h) Reconnection Testing and Approval

OCC's proposed changes would adopt Rule 213(h) titled "Reconnection Testing and Approval, " which would require, prior to any Reconnection, that the subject Clearing Member must demonstrate, as applicable, to OCC's reasonable satisfaction, that it: (i) can operate in a test environment, including, but not limited to, sending and receiving messages and transactions; (ii) can replay or resubmit previously submitted messages or transactions; (iii) can reverse or void previously submitted messages or transactions; (iv) can confirm the integrity of messages and transactions; (v) has alternative communication methods with OCC to facilitate the exchange of messages, transactions, and reports; and (vi) can complete any other such requirements as are reasonably requested by OCC. Furthermore, proposed Rule 213(h)(2) would authorize two or more Designated Officers of OCC to, in their reasonable judgment, approve the Reconnection of a Clearing Member that was the subject of action taken pursuant to proposed Rule 213, after OCC has received all required information pursuant to this Rule, in a form and a substance satisfactory OCC, and that all information necessary for a safe Reconnection and certain testing has occurred, pursuant to proposed Rule 213(h)(1).

The purpose of proposed Rule 213(h) is to ensure that the approval for a Reconnection is not made until OCC has received, to its satisfaction, all necessary

information from the Clearing Member, and that OCC confirmed the subject Clearing Member can safely perform the capabilities necessary for submitting, receiving, and correcting information appropriately and in a manner unaffected by the Clearing Member System Event, so as to help mitigate the risk presented by the Reconnection. In addition, OCC believes it is appropriate that the approval of a Reconnection be made by at least two members of OCC's management committee to help ensure that information regarding the Reconnection has been escalated to the highest management level.

Proposed Rule 213(i) Certain Miscellaneous Matters

OCC proposes to adopt Rule 213(i), titled "Certain Miscellaneous Matters," which would address various provisions including, but not limited to, (i) OCC's limited liability to a Clearing Member pursuant to proposed Rule 213; (ii) OCC's authority to inform the subject Clearing Member's Third-Party Service Provider, or require the Clearing Member to inform its Third-Party Service Provider, of a Clearing Member System Event; and (iii) the failure of a Clearing Member to comply with proposed Rule 213.

First, in an effort to promote enhanced transparency to Clearing Members, proposed Rule 213(i)(1) would address, in part, OCC's limited liability to any Clearing Member as it relates to losses arising out of OCC's action or inaction pursuant to proposed Rule 213. More specifically, proposed Rule 213(i)(1) would provide that without limiting any other provisions in these Rules concerning limitations on liability, neither OCC nor its directors, officers, employees, agents, or contractors shall be liable to any Clearing Member or any customer or client thereof for: (i) any failure, hindrance, interruption or delay in performance in whole or in part of the obligations of OCC under

these Rules, if that failure, hindrance, interruption or delay arises out of or relates to a Clearing Member System Event, Major Clearing Member System Event, or any action or inaction pursuant to this Rule 213; or (ii) any loss, liability, damage, cost or expense arising from or relating in any way to any advice, request, requirement, instruction, action or inaction pursuant to this Rule 213.²⁰ Second, proposed Rule 213(i)(2) would provide that the power of OCC to take any action pursuant to this Rule 213, or to request or require any action, documentation, or information pursuant to this Rule 213, also includes the power to waive, repeal, rescind, revoke, amend, or vary any such action, request, or requirement in consideration of the facts and circumstances. Third, proposed Rule 213(i)(3) would provide that the powers of OCC pursuant to this Rule 213 are in addition to, and not in limitation of, any authority granted elsewhere in these Rules to act as specified therein. The purpose of proposed Rule 213(i)(2) and proposed Rule 213(i)(3) is to promote enhanced transparency to Clearing Member on OCC's authority to take action pursuant to Rule 213 so that Clearing Members can better understand and be prepared for their obligations to OCC.

Fourth, proposed Rule 213(i)(4) would provide that all information related to or regarding a Major Clearing Member System Event and all acts pursuant to this Rule 213 will be considered Confidential Information pursuant to these Rules; provided, however, that the OCC may inform, or direct the Clearing Member to inform, the Clearing Member's Third-Party Service Provider of a Clearing Member System Event if OCC determines, in its discretion, that such action is necessary for the protection of OCC and

²⁰ The provisions described in (i) through (ii) would be organized as proposed Rule 213(i)(1)(A) through 213(i)(1)(B).

other Clearing Members. The purpose of the proposed change is to mitigate risk to OCC and its Clearing Members that may be presented by a Clearing Member System Event and associated Major Clearing Member System Event. The proposed changes also provide transparency to Clearing Members on their obligation to inform their Third-Party Service Providers in certain circumstances that OCC deems necessary.

Fifth, proposed Rule 213(i)(5) would provide that the failure of a Clearing Member to comply with the requirements of this Rule 213 may subject the Clearing Member to any and all disciplinary action permitted under these Rules, including, without limitation, suspension. Lastly, proposed Rule 213(i)(6) would provide that a Clearing Member that has authorized another party, such as a Third-Party Service Provider, to access and use OCC's systems will be responsible for such authorized party's compliance with the requirements of this Rule 213 and any compliance failure by that authorized party will be deemed to be a failure of the authorizing Clearing Member. The purpose of proposed Rules 213(i)(5) and 213(i)(6) is to highlight the importance of complying with proposed Rule 213 and the actions OCC may take if there is a failure to comply.

2. Statutory Basis

OCC believes the proposed rule change is consistent with Section 17A of the Exchange Act²¹ and Rule 17ad-22(e)(2) and (e)(17)²² thereunder. Section 17A(b)(3)(F) of the Act²³ requires, among other things, that the rules of a clearing agency be designed to promote the prompt and accurate clearance and settlement of securities transactions, and

²¹ 15 U.S.C. 78q-1.

²² 17 CFR 240.17ad-22(e)(2) and (e)(17).

²³ 15 U.S.C. 78q-1(b)(3)(F).

to assure the safeguarding of securities and funds which are in the custody or control of the clearing agency or for which it is responsible. OCC's proposed amendments to Rule 213 are designed to help OCC assess and take appropriate action to manage the cybersecurity risks that may be introduced to OCC's Systems and information due to a Clearing Member System Event. The proposed changes to Rule 213 enhance OCC's processes to help mitigate risk and better protect OCC and its Clearing Members.

As described above, the proposed rule change would, in part: (i) introduce a defined terms section to Rule 213 that broadens the definition of OCC Systems to include established communication channels, such as FTPs, in addition to direct connections; (ii) require that the Cybersecurity Confirmation be signed by a senior executive of the Clearing Member or applicant who is authorized to attest to such matters; (iii) remove language inviting a Clearing Member to assess the potential impact of a Clearing Member System Event on OCC's systems and operations when determining whether the event is reportable, and instead specify the timeframe for reporting such an event and the specific information that must be included in the notice; (iv) establish the concept of a "Major Clearing Member System Event," including a declaration process requiring approval by two or more Designated Officers and prompt notification to the Chairman of the Board; (v) reorganize and clarify OCC's authority to take action in response to a Clearing Member System Event, including specifying the actions that constitute a "disconnect" and clarifying a Clearing Member's related obligations; (vi) add provisions establishing the reporting, testing, approval, and governance requirements necessary for reconnection, including OCC's ability to require an audit report from a Third-Party Cybersecurity Firm; and (vii) provide OCC with the authority to inform, or to require a

Clearing Member to inform, the Clearing Member's Third-Party Service Provider of a Clearing Member System Event if OCC determines, in its discretion, that such action is necessary to protect OCC and other Clearing Members. OCC believes that these proposed changes will enhance Rule 213 to be more efficient, effective and clear in the cybersecurity obligations of its Clearing Members so that OCC may better address cybersecurity risks to protect OCC and its Clearing Members. Among the amendments discussed above, OCC believes the following amendments to Rule 213 are particularly consistent with the requirements of Section 17A(b)(3)(F) of the Act, as discussed in further detail below: (i) expanded notification requirements applicable to a Clearing Member System Event; (ii) the establishment of the Major Clearing Member System Event and its related governance; and (iii) the process for Reconnection of a Clearing Member.

First, proposed Rule 213(d) codifies within OCC's rules the specific content and timeframe requirements for notification of a Clearing Member System Event, which OCC believes is consistent with the requirements of Section 17A(b)(3)(F) of the Act.²⁴ Under proposed Rule 213(d), a Clearing Member would be required to provide OCC with specified information at the onset of a Clearing Member System Event, including but not limited to the event type, effect, scope, start date, end date, discovery date, and any public notices related to the event. OCC believes this requirement will allow OCC to receive consistent, timely information from Clearing Members, which in turn, will help to minimize the risk that delayed or incomplete information impacts OCC's ability to respond promptly and effectively to such events. As such, OCC believes this proposed

²⁴Id.

change supports the prompt and accurate clearance and settlement of securities transactions and assures the safeguarding of securities and funds that are in the custody or control of OCC, consistent with Section 17A(b)(3)(F) of the Act.²⁵

Second, proposed Rule 213(e) establishes the concept of a “Major Clearing Member System Event,” which OCC believes is also consistent with the requirements of Section 17A(b)(3)(F) of the Act.²⁶ Under proposed Rule 213(e), OCC would assess the potential impact of a Clearing Member System Event on OCC’s Systems and operations, and would determine to act, or refrain from acting, depending on the specific details of the event. This removes the ambiguity that may exist in the current rule text, which instead invites the Clearing Member to assess potential impact of its own Clearing Member System Event on OCC’s Systems or operations. Furthermore, under proposed Rule 213(e), the existence of a Major Clearing Member System Event must be declared by two or more Designated Officers of OCC, in their reasonable judgement. Following such a declaration, OCC will promptly notify the Chairman of the Board. OCC believes this process ensures that the most severe threats to OCC’s Systems and operations are escalated to the highest levels of OCC’s governance. OCC believes the establishment of a Major Clearing Member System Event and the governance outlined in proposed Rule 213(e) is consistent with Section 17A(b)(3)(F) of the Act because OCC, not the reporting Clearing Member, is best positioned to determine the severity of a threat to OCC’s own Systems and operations. Additionally, OCC believes that escalation to the highest levels of OCC’s governance helps to ensure events with the greatest potential impact to OCC

²⁵ Id.

²⁶ Id.

receive attention and oversight proportionate to their severity. As such, OCC believes the proposed rule change is designed to assure the safeguarding of securities and funds in the custody or control of OCC, consistent with the requirements in Section 17A(b)(3)(F) of the Act.²⁷

Third, proposed Rule 213(h) establishes reconnection testing and approval requirements that OCC believes are consistent with Section 17A(b)(3)(F) of the Act. Under proposed Rule 213(h)(1), prior to Reconnection, a Clearing Member must demonstrate, to OCC's reasonable satisfaction, that it can, in part, operate in a test environment, send and receive messages and transactions, replay or resubmit previously submitted messages or transactions, reverse or void previously submitted messages or transactions, confirm the integrity of messages and transactions, and maintain alternative communication methods with OCC. These requirements test the Clearing Member's operational capability to interact accurately and reliably with OCC's Systems, rather than relying on the Clearing Member's representation that it is prepared to reconnect. OCC believes this proposed change is designed to safeguard securities and funds in the custody or control of OCC by verifying, before Reconnection occurs, that a Clearing Member's systems will not transmit corrupted or otherwise unreliable messages or transactions into OCC's Systems and operations. As such, OCC believes this proposed change is designed to assure the safeguarding of securities and funds in the custody or control of OCC, consistent with the requirements in Section 17A(b)(3)(F) of the Act.²⁸

²⁷ Id.

²⁸ Id.

Risks presented by a Clearing Member System Event could impact OCC's ability to clear and settle securities transactions, or to safeguard the securities and funds that are in its custody or control, or for which it is responsible. Therefore, by enhancing OCC's processes to mitigate these risks, including but not limited to: expanding the notification requirements, establishing the concept of a Major Clearing Member System Event, and enhancing its process for Reconnection, OCC believes the proposed changes would promote the prompt and accurate clearance and settlement of securities transactions and assure the safeguarding of securities and funds that 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.²⁹

Consistency with Rule 17ad-22(e)(2)(i) and (v)

OCC believes the proposed changes to Rule 213 are consistent with Rule 17ad-22(e)(2)(i) and (v), which require, in part, that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to provide for governance arrangements that (i) are clear and transparent and (ii) specify clear and direct lines of responsibility.³⁰ OCC specifies in proposed Rule 213(e)(1) that the existence of a Major Clearing Member System Event must be declared by two or more Designated Officers of OCC, and OCC will provide notification of such declaration to the Chairman of the Board. Proposed Rule 213(e)(1) establishes a defined pathway from identification of the event, through declaration by two or more Designated Officers, to notification at the Board level. As such, OCC believes this specificity is consistent

²⁹ Id.

³⁰ 17 CFR 240.17ad-22(e)(2)(i) and (v).

with the “clear and transparent” governance arrangements required by Rule 17Ad-22(e)(2)(i). It is likewise consistent with the “clear and direct lines of responsibility” required by Rule 17Ad-22(e)(2)(v), because this proposed change assigns responsibility for determining a Major Clearing Member System Event to a specifically identified group of officers.

Similarly, with respect to Reconnection, proposed Rule 213(h)(2) requires that the Reconnection of a Clearing Member following OCC’s action pursuant to proposed Rule 213(f)(1) be approved by two or more Designated Officers of OCC, and conditions that approval on OCC’s receipt of all information required under Rule 213, in a form and substance satisfactory to OCC, and satisfaction of the applicable testing requirements set forth in proposed Rule 213(h)(1). By specifying both who is authorized to approve Reconnection and the steps that must be satisfied before that approval may be granted, proposed Rule 213(h)(2) establishes a transparent and structured approval process, consistent with Rule 17Ad-22(e)(2)(i). It also identifies, with the same specificity as the Major Clearing Member System Event declaration process, the officers responsible for making a determination to reconnect a Clearing Member, consistent with the clear and direct lines of responsibility required by Rule 17Ad-22(e)(2)(v). Therefore, OCC believes the proposed changes are consistent with Rule 17ad-22(e)(2)(i) and (v) under the Act.³¹

Consistency with Rule 17ad-22(e)(17)(i)

OCC believes the proposed changes to Rule 213 are also consistent with Rule 17ad-22(e)(17)(i) under the Act, which requires that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably

³¹ Id.

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.³²

As described above, the proposed changes to Rule 213, in part: (i) enhance the requirements of Clearing Members to notify OCC in the event of a Clearing Member System Event; (ii) add provisions around reporting, testing and approval requirements, and governance necessary for Reconnection of a Clearing Member, in the event OCC takes action pursuant to proposed Rule 213(f)(1); and (iii) update and add definitions for purposes of Rule 213 to clarify the obligations of a Clearing Members and its Third-Party Service Providers.

First, OCC believes the enhancements notification requirements in proposed Rule 213(d) are consistent with the requirements set forth in Rule 17Ad-22(e)(17)(i).³³ Proposed Rule 213(d) outlines the requirements applicable to a Clearing Member's notification of a Clearing Member System Event to OCC. This includes removing language that invites a Clearing Member to assess the potential impact of the event on OCC's Systems and operations in determining whether the event was reportable, specifying the timeframe within which such an event must be reported, and identifying the specific information that must be included in the notice. OCC believes these enhancements are consistent with Rule 17Ad-22(e)(17)(i), which requires OCC to identify the plausible sources of its operational risk, both internal and external. Because a Clearing Member System Event represents an external source of potential operational

³² 17 CFR 240.17ad-22(e)(17)(i).

³³ Id.

risk to OCC, OCC's ability to identify and characterize that risk depends on receiving timely, complete, and accurate information from the Clearing Member. The specified content requirements, including but not limited to, the event type, effect, scope, and start, end, and discovery dates, further support OCC's ability to identify the nature and extent of the risk presented. As such, OCC believes the proposed change helps OCC to identify, in a timely manner, plausible sources of operational risk presented by a Clearing Member System Event, and mitigate risk presented to OCC and its Clearing Members, consistent with Rule 17ad-22(e)(17)(i).³⁴

Second, OCC's proposed changes in Rule 213(h) enhance the requirements surrounding the Reconnection of a Clearing Member, which will help OCC evaluate and determine whether Reconnection is appropriate and, if so, take steps to ensure a safe Reconnection. OCC believes these enhancements are also consistent with the requirements in Rule 17Ad-22(e)(17)(i) of the Act³⁵ that requires OCC to identify and mitigate the impact of its operational risks through appropriate systems, policies, procedures, and controls. Proposed Rule 213(h)(1) requires that, prior to Reconnection, a Clearing Member demonstrate, to OCC's reasonable satisfaction, that it can operate in a test environment, replay or resubmit previously submitted messages or transactions, reverse or void previously submitted messages or transactions, confirm the integrity of messages and transactions, and maintain alternative communication methods with OCC. OCC believes is consistent with the requirements in Rule 17Ad-22(e)(17)(i) because the proposed change identifies, through testing requirements, whether the specific risks

³⁴ Id.

³⁵ Id.

presented by the original Clearing Member System Event, including, for example, data loss or communication failure, have been resolved. By requiring the Clearing Member to demonstrate these capabilities before Reconnection is granted, proposed Rule 213(h)(1) mitigates the risk that reconnecting the Clearing Member would reintroduce the same operational risk to OCC's Systems that necessitated the disconnection in the first place. In addition, under proposed Rule 213(g)(3), OCC can request a detailed, comprehensive, and auditable report from a Third-Party Cybersecurity Firm, either as a condition to or following Reconnection. This report must include, but is not limited to, a timeline of the Clearing Member System Event, a description of the event and how it was corrected or resolved, a root cause analysis, confirmation that any issues identified as severe, critical, or moderate have been resolved, confirmation that the affected systems have returned to normal, pre-incident operation for at least 72 hours, and short and long-term preventive monitoring and detection recommendations. OCC's ability to require an audit report from a Third-Party Cybersecurity Firm will enable OCC to collect and evaluate information from a reputable source to help OCC determine whether to reconnect. The requirement for an independent root cause analysis supports OCC's identification of the operational risk's underlying cause, while the requirement for verified confirmation supports the rule's mitigation component. As such, OCC believes this proposed change is consistent with the requirements in Rule 17Ad-22(e)(17)(i).³⁶

Third, OCC believes the proposed addition of a defined terms section to Rule 213, including an expanded definition of OCC's Systems to encompass established communication channels, such as FTPs, that may be used to transmit data or instructions

³⁶Id.

to a Clearing Member's back-office systems, is consistent with Rule 17Ad-22(e)(17)(i) of the Act.³⁷ OCC believes that expanding the definition of OCC's Systems to include these indirect channels is appropriate because a security intrusion can reach OCC through such a channel, in addition to a direct connection, so OCC believes it is prudent to codify this in its rules to help identify that potential source of risk. OCC's proposed changes also update the definition of a "Clearing Member System Event" to include an incident resulting from a Clearing Member's Third-Party Service Provider connected to OCC's Systems. By establishing definitions for these terms and, more specifically, expanding the definition of Clearing Member System Event to incorporate the Clearing Member's Third-Party Service Provider, this will help OCC to better identify and manage risks presented by a Clearing Member or its Third-Party Service Provider connected to OCC's Systems.

By enhancing reporting and notification requirements for Clearing Members in the event of a Clearing Member System Event, strengthening the testing, reporting, approval and governance requirements surrounding reconnection of a Clearing Member, and adding and updating definitions for the purpose of proposed Rule 213, OCC believes such changes will help to identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls, in accordance with Rule 17ad-22(e)(17)(i).³⁸

Consistency with Rule 17ad-22(e)(17)(ii)

³⁷ Id.

³⁸ Id.

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.³⁹ In addition to OCC's existing process that requires a Reconnection Attestation and Checklist to be submitted by a Clearing Member that has been disconnected, OCC's proposed changes to Rule 213 add provisions to strengthen the overall process and requirements around Reconnection of a Clearing Member. These changes include, but are not limited to: (i) the requirement that the subject Clearing Member submit the Reconnection Attestation prior to OCC reestablishing connectivity; (ii) the obligation for the subject Clearing Member to complete specific testing requirements prior to Reconnection in order to demonstrate to OCC that it is operationally ready to reconnect; and (iii) OCC's ability to request a report from a Third-Party Cybersecurity Firm, either as a condition to Reconnection or following Reconnection. By requiring that the subject Clearing Member (i) submit the Reconnection Attestation prior to OCC reestablishing connectivity, and (ii) complete specific testing requirements prior to OCC reestablishing connectivity, OCC will be able to better identify and address potential vulnerabilities that may still exist within the Clearing Member's environment after a Clearing Member System Event has occurred, and take steps to promote resiliency prior to establishing Reconnection. Furthermore, by including the ability for OCC to require an audit report from a Third-Party Cybersecurity Firm, OCC will be provided with key details about the Clearing Member System Event from a reputable and experienced source. OCC will be

³⁹

17 CFR 240.17ad-22(e)(17)(ii).

able to rely upon the information in the report to help analyze and address the Clearing Member System Event in effort to further mitigate risk. This, in turn, helps to strengthen OCC's security protocols. OCC believes these proposed changes provide OCC with the necessary tools to address and manage OCC's operational risks by ensuring, in part, that systems have a high degree of security, resiliency, and operational reliability, in accordance with Rule 17ad-22(e)(17)(ii).⁴⁰

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

Section 17A(b)(3)(I) of the Act⁴¹ 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 Rule 213 in effort to strengthen OCC's security protocols and promote resiliency when confronted with cybersecurity risks presented by OCC's interconnections with its Clearing Members. OCC believes the three of the proposed changes could have an impact on competition, but such impact is necessary and appropriate in further of the purposes of the Act. The three proposed changes that OCC believes could have an impact on competition include: (i) adding the definition of a Third-Party Service Provider in proposed Rule 213(a)(6) to include an affiliate of any Clearing Member, service bureau or similar entity that connects to OCC's Systems on behalf of or for the benefit of a Clearing Member; (ii) adopting proposed Rule 213(g)(3), which provides OCC with the ability to require an audit report from a

⁴⁰ Id.

⁴¹ 15 U.S.C. 78q-1(b)(3)(I).

Third-Party Cybersecurity Firm; and (iii) establishing the requirements for testing prior to reconnection of a Clearing Member, as described in proposed Rule 213(h). As described below, although the three proposed changes may have an impact on competition, OCC believes that such impact is necessary and appropriate in further of the purposes of the Act.

Proposed Rule 213(a) establishes the definition of “Third-Party Service Provider” to include an affiliate of any Clearing Member, service bureau or similar entity, that connects to OCC’s Systems on behalf of or for the benefit of a Clearing Member. Establishing the definition of Third-Party Service Provider for purposes of Rule 213 to include such entities described above could impose a burden on competition because such entities would now be explicitly subject to the requirements in Rule 213, including disconnection and Reconnection requirements. OCC acknowledges that being disconnected from OCC’s Systems may impact the entity’s ability to perform certain functions, therefore putting the entity at a competitive disadvantage. However, OCC believes that the proposed change would not create a significant burden. Based on OCC’s critical role as a SIFMU, OCC has the responsibility to promote financial stability and protect the broader marketplace. Due to the close relationship and interconnectivity that exists between a Third-Party Service Provider and the related Clearing Member, OCC believes that it is critical to address risks presented by the Third-Party Service Provider that connects to OCC’s Systems on behalf of or for the benefit of a Clearing Member. Although this proposed change may impose a burden on such entity, OCC does not believe this burden is significant, and as described in proposed Rule 213(f)(1)(C), OCC would, as appropriate and practical, seek to facilitate the continuation of services for an

entity that is subject to a Clearing Member System Event. Therefore, OCC believes the burden on competition is necessary and appropriate in furtherance of the purposes of the Act.

Proposed Rule 213(g)(3) provides OCC with the ability to require that the Clearing Member must provide an audit report from a Third-Party Cybersecurity Firm, either as a condition to Reconnection or following a Reconnection. Although this requirement may impose a burden on competition, OCC does not believe this burden is significant. As described above, given OCC's role as a SIFMU and its position in the marketplace, OCC believes it is prudent to enhance its management of Clearing Member System Events. OCC believes the ability to require, in certain circumstances, that the Clearing Member provide an audit report from a Third-Party Cybersecurity Firm will provide OCC with key details about the Clearing Member System Event. OCC believes this will help OCC analyze such incident and take necessary steps to mitigate risks presented. Although the Clearing Member may incur additional costs through the requirement to provide such audit report from a Third-Party Cybersecurity Firm, OCC believes this proposed change would not present an undue burden. OCC would also expect Clearing Members to leverage their existing relationships with Third-Party Cybersecurity Firms in effort to reduce costs of providing such audit report. OCC believes the proposed change is necessary to promote resiliency and enhance OCC's security protocols to protect OCC and Clearing Members from cybersecurity risks. Therefore, OCC believes the burden on competition presented by the proposed change is necessary and appropriate in furtherance of the Act.

OCC believes proposed Rule 213(h), which establishes testing requirements for Clearing Members prior to reconnection, may impose a burden on competition on a Clearing Member because the changes create additional steps that the Clearing Member must complete prior to reconnection. OCC acknowledges that these additional steps, if not completed by the Clearing Member, could result in a Clearing Member being disconnected from OCC's System's for a longer period of time than the Clearing Member would have expected, which may impose a burden on the Clearing Member. However, OCC believes that the burden on competition from the proposed testing requirements is necessary to help ensure that Reconnection is safe and appropriate. The purpose of the proposed testing requirements is to strengthen OCC's security protocols so that OCC can identify any vulnerabilities related to a Clearing Member System Event prior to establishing any Reconnection. Although this proposed change may impose a burden on the Clearing Member, OCC does not believe this burden is significant. In addition, proposed Rule 213(f)(1)(C), also provides that OCC will, as appropriate and practical, seek to facilitate the continuation of services of a disconnected Clearing Member, prior to Reconnection. Therefore, OCC believes the proposed change requiring testing requirements prior to Reconnection of a Clearing Member is necessary to help mitigate risk presented and ultimately protect OCC and other Clearing Members.

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 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-2026-010 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-2026-010. 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 such filing 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>.

Do not include personal identifiable information in submissions; you should submit only information that you wish to make available publicly. We may redact in part or withhold entirely from publication submitted material that is obscene or subject to copyright protection.

All submissions should refer to File Number SR-OCC-2026-010 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.⁴²

Secretary

⁴²

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

Exhibit 3

This Exhibit contains electronic files embedded in this cover page for filing efficiency, as identified below. OCC has omitted the embedded file pursuant to 17 CFR 240.24b-2. OCC has separately filed and requested confidential treatment of the cover page containing the embedded file as protected from public disclosure by Exemptions 4 and 8 of the Freedom of Information Act (“FOIA”), 5 U.S.C. 552(b)(4), (b)(8), and 15 U.S.C. 78x(e) because the information it contains concerns (i) OCC’s trade secrets and commercial information not customarily released to the public and is, and always has been, treated as the private information of OCC, the release of which is likely to cause foreseeable harm to OCC’s commercial or financial interests; and (ii) the supervision of OCC, a financial institution regulated by the Commission. OCC believes the Form 19b-4 Information and Exhibit 1A provide a clear and adequate description of the relevant substance of the embedded files to facilitate meaningful public comment.

Embedded File: [Redacted Pursuant to Rule 24b-2]

- OCC’s Information Security Disconnection and Reconnection Procedure [Confidential]; 12 pages

EXHIBIT 5



OCC Rules

Blue underlined text indicates additions

~~Red strikethrough~~ text indicates deletions

~~Green double-strikethrough~~ indicates deletions to existing Rule 213 that are being relocated within OCC's Rules, as indicated by green underlined text and in [brackets]

RULE 213 – Cybersecurity Obligations

(a) Defined Terms. For purposes of this Rule 213, the following terms have the following meanings:

(1) “Best Practices” means policies, procedures, practices or similar standards and guidelines that are reasonably designed and consistent with then current financial- sector cybersecurity standards issued by an authoritative body that is a U.S. governmental entity or agency, an association of a U.S. governmental entity or agency, or a widely recognized industry organization.

(2) “Clearing Member System Event” means an incident resulting from the unintended or unauthorized access to, or the malfunction or corruption (whether partial or total) of one or more systems, of a Clearing Member or its Third-Party Service Provider, connected to the Corporation’s Systems.

(3) The “Corporation’s Systems” means the systems, equipment and technology networks of the Corporation, whether owned, leased, or licensed, and including software, hardware, applications, devices, IP addresses, or other addresses or accounts used in an established communication channel with such systems, equipment and technology networks, to provide the services set forth in these Rules, or otherwise used to transact business or connect with the Corporation.

(4) “Major Clearing Member System Event” means a Clearing Member System Event that has or is reasonably anticipated to, for example, disrupt, degrade, cause a delay in, interrupt or otherwise alter the normal operation of the Corporation’s Systems; result in unauthorized access to the Corporation’s Systems; result in the loss of control of, disclosure of, or loss of the Corporation’s Confidential Information; or cause a strain on, loss of, or overall threat to the Corporation’s resources, functions, security or operations.

(5) “Third-Party Cybersecurity Firm” means a firm that, in the Corporation’s reasonable judgement, (A) (i) is well-known and reputable; (ii) is not the subject Clearing Member, or an affiliate or a Third-Party Service Provider of the subject Clearing Member; (iii) is experienced in financial-sector cybersecurity; and (iv) employs Best Practices; or (B) is otherwise determined to be a Third-Party Cybersecurity Firm by the Corporation.

(6) “Third-Party Service Provider” means an affiliate of any Clearing Member, service bureau or other similar entity, that connects to the Corporation’s Systems on behalf of or for the benefit of a Clearing Member.

(a**b**) Cybersecurity Confirmation Submission.

(1) Each Clearing Member ~~and applicant for clearing membership shall~~ must complete and submit an attestation ~~form, provided by the Corporation,~~ at least every two years, and not later than 180 calendar days from the date that the Corporation notifies the Clearing Member that the attestation is required, that confirms the existence of an information system cybersecurity program and includes required representations as determined by the Corporation (“Cybersecurity Confirmation”).

~~(i)~~(2) Each applicant for clearing membership shall must 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 the Corporation notifies the Clearing Member that an attestation is required.~~

(~~b~~c) *Representations in the Cybersecurity Confirmation.* The Cybersecurity Confirmation ~~shall~~must be signed by a senior executive of the Clearing Member or applicant who is authorized to attest to these matters and 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. 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 ~~t~~Third-~~p~~Party ~~s~~Service ~~p~~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~~i) evaluate the cyber risks and impact of these third parties, and (~~B~~i) 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:
 - ♦ (~~A~~A) 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;
 - ♦ (~~B~~B) 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;
 - ♦ (~~C~~C) 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
 - ♦ (~~D~~D) 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 Clearing Member System Event* ~~Security Incident~~. A Clearing Member experiencing a Clearing Member System Event must notify the Corporation immediately in writing, but no later than two (2) hours, ~~and shall promptly confirm such notice in writing if the~~ after the Clearing Member becomes aware or should be aware that there has been an Clearing Member System Event incident, or a incident is occurring, involving a cyber related disruption or intrusion of the Clearing Member's system(s) that is reasonably likely to pose an imminent risk or threat to the Corporation's operations. Such occurrence A Clearing Member System Event may include, but is not limited to, any disruption or degradation of the normal operation of the Clearing Member's system(s) or any unauthorized entry into the Clearing Member's system(s) that would result in loss of the Corporation's data or system integrity, unauthorized disclosure of sensitive information related to the Corporation, or the inability of the Corporation to conduct essential clearance and settlement functions ~~("Security Incident")~~. Notification pursuant to this section must, at a minimum include the following information, and any such information unconfirmed or otherwise unknown may be identified by the Clearing Member as "Unknown":

(1) Legal Entities. A complete list of the legal entity names of the Clearing Member and any Third-Party Service Providers experiencing or otherwise affected or potentially affected by the Clearing Member System Event.

(2) Contact Information. A list of persons – with their corresponding titles, primary email addresses and phone numbers, and, if those primary email addresses and phone numbers are associated with the systems that are the subject of the Clearing Member System Event, alternate email addresses and phone numbers – who are authorized to act on behalf of the subject Clearing Member regarding the Clearing Member System Event.

(3) Clearing Member System Event Details:

- ♦ (A) Event Type – the type of Clearing Member System Event, for example, an insider threat, phishing attack, MITM attack, privilege escalation, denial of service, external threat, malware, unauthorized access, ransomware, compromised user account, SQL injections, brute force attack, system compromise, supply chain attacks (as each term is commonly understood by cybersecurity professionals in the financial sector), or other – if other, please explain.
- ♦ (B) Event Effect - perceived, anticipated, or known effect of the Clearing Member System Event, for example, loss of communication, data corruption, security breach, or other – if other, please explain.
- ♦ (C) Start Date – date and time when the Clearing Member System Event began.
- ♦ (D) End Date – date and time when the Clearing Member System Event ended, if applicable.
- ♦ (E) Discovery Date – date and time when the Clearing Member System Event was first identified.

- (F) Scope – scope of the Clearing Member System Event, including, but not limited to, a list of each affected or likely affected system or data, including the Corporation’s Systems and data, the degree of such affect, and any supporting evidence of such.
- (G) Notices – whether any formal or informal notices or information regarding the Clearing Member System Event was made public and, if so, provide a copy of such notices or information.

(e) Declaration of a Major Clearing Member System Event.

(1) Upon becoming aware of a Clearing Member System Event, the Corporation will consider whether such Clearing Member System Event meets the definition of a Major Clearing Member System Event. The existence of a Major Clearing Member System Event must be declared by two or more Designated Officers of the Corporation, in their reasonable judgement.

(2) Upon declaration of a Major Clearing Member System Event, the Corporation may act (or refrain from acting) pursuant to this Rule to help address, correct, mitigate or alleviate any and all risks presented to the Corporation by or related to the Major Clearing Member System Event. Action taken will be in consideration of the risks presented to the Corporation, including but not limited to, information provided pursuant to this Rule.

(3) Following declaration of a Major Clearing Member System Event, the Corporation will promptly notify the Chairman of the Board of Directors of such declaration.

(f) Authority to Take Action and Required Cooperation.

(1) Upon ~~such~~ notice of a Clearing Member System Event, or if the Corporation has a reasonable basis to believe that a Clearing Member System Event ~~Security Incident~~ has occurred, or is occurring, the Corporation may take actions reasonably necessary to mitigate any effects to its operations, including to:

(A) ~~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 s~~Systems;

(B) suspend any and all transmissions, communications, or access between the Corporation’s Systems (together with actions taken under Rule 213(f)(1)(A), “disconnect”); or

(C) take, or refrain from taking, or require the subject Clearing Member to take or refrain from taking, any and all action that the Corporation considers appropriate to help address, correct, mitigate or alleviate the Major Clearing Member System Event and, as appropriate and practical, facilitate the continuation of services, which may include issuing instructions to the subject Clearing Member and requiring such Clearing Member to act on such instructions.

(2) In determining whether to disconnect a Clearing Member, the Corporation will evaluate the facts and circumstances related to the Clearing Member System Event ~~Security Incident~~. The Corporation may take into consideration a number of factors, including, but not limited to, the potential loss of control by a Clearing Member of its internal system(s), the potential loss of the Corporation’s confidential data, the potential strain on or loss of the Corporation’s resources due to the Corporation’s inability to perform clearance and settlement functions, and the overall severity of the threat to the security and operations of the Corporation.

(3) The Corporation will promptly notify the Clearing Member of any disconnect or other material action the Corporation takes with respect to such Clearing Member pursuant to this Rule.

Notwithstanding any action taken pursuant to this Rule, ~~If the Corporation determines that disconnection of a Clearing Member is necessary~~, the Clearing Member must continue to meet its obligations to the Corporation, and comply with the statutory rules of the Corporation, as defined in its By-Laws. ~~notwithstanding disconnection from the Corporation's systems.~~

(4) The Clearing Member must cooperate fully and completely with, and to the reasonable satisfaction of, the Corporation in all matters relating to the Major Clearing Member System Event, including, but not limited to:

(A) conducting timely investigations and inquiries, as the Corporation believes reasonably necessary, with respect to any known or unknown information relating to the Clearing Member System Event;

(B) promptly notifying the Corporation of any material changes, updates, or new information learned regarding the Clearing Member System Event; and

(C) promptly providing any documentation or information requested by the Corporation, unless not legally permitted to do so, regarding or related to the Clearing Member System Event.

(eg) Procedures for ~~Connecting-Reconnection~~ ~~Following a Security Incident that Results in Disconnection.~~

(1) Reconnection Attestation. ~~In the event If the Corporation OCC disconnects-takes action pursuant to Rule 213(f)(1) a Clearing Member that has reported a Security Incident, upon the request of the Corporation,~~ the Clearing Member must complete and submit a form as provided by the Corporation that describes the Clearing Member System Event ~~Security Incident~~ and includes required representations ("Reconnection Attestation") prior to the Corporation reestablishing connectivity to the Corporation's Systems ("Reconnection"). ~~The Clearing Member also will be required to complete an associated checklist as provided by the Corporation that describes remediation efforts ("Reconnection Checklist").~~ ~~(1) Representations in the Reconnection Attestation.~~ The Reconnection Attestation must be signed by a ~~designated~~ senior executive of the Clearing Member who is authorized to attest to the representations required therein, including, but not limited to, the following:

(A) the Clearing Member has provided full, complete and accurate information in response to all requests made by the Corporation regarding the Clearing Member System Event ~~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 Clearing Member System Event ~~Security Incident~~, including any potential exposure of credentials used to access the Corporation's ~~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 Clearing Member System Event ~~Security Incident~~;

(C) the Clearing Member has determined whether the Clearing Member System Event ~~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 Clearing Member System Event 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 Clearing Member System Event Security Incident, including any notifications required to be provided to government agencies, the Corporation, and third parties.

(2) Reconnection Check-List. If the Corporation takes action pursuant to Rule 213(f)(1), the Clearing Member ~~also will be required to~~ must complete an associated checklist as provided by the Corporation that describes remediation efforts (“Reconnection Checklist”), which may require information including but not limited to:-

[Text relocated from current Rule 213(e)]

(A) ~~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;

(B) the nature of the incident;

(C) the steps taken to contain the incident;

(D) the data of the Corporation, if any, that was compromised during the incident;

(E) the systems of the Corporation, if any, that were impacted during the incident;

(F) 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;

(G) 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;

(H) details on how data integrity has been preserved and what data checks have been performed;

(I) whether third-parties, including government agencies, have been notified; and

(J) any additional details relevant to Recconnection.

(3) Report from Third-Party Cybersecurity Firm. If the Corporation takes action pursuant to Rule 213(f)(1), the Corporation may require, either as a condition to Reconnection or following Reconnection, that the Clearing Member provide a detailed, comprehensive, and auditable report from a Third-Party Cybersecurity Firm, or summary of such report, that includes:

(A) a timeline of the Clearing Member System Event, including all material actions, events, and decisions taken for or relating to the Clearing Member System Event;

(B) a description of the Clearing Member System Event and an explanation of how such disruption was corrected or resolved;

(C) root cause analysis of the Clearing Member System Event;

(D) confirmation that any issues identified by the Third-Party Cybersecurity Firm as severe, critical, or moderate, or comparable categorizations, have been resolved;

(E) confirmation of normal or intended operation of the subject system(s), including, but not limited to, the return or replacement of key systems and data stores to pre-Clearing Member System Event resilience, in a safe, secure and proper manner for at least 72 hours;

(F) a description of short- and long -term preventive monitoring and detection recommendations from the Third-Party Cybersecurity Firm; and

(G) any other information reasonably requested to be included by the Corporation.

(h) Reconnection Testing and Approval.

(1) Prior to any Reconnection pursuant to this Rule, the subject Clearing Member must demonstrate, as applicable, to the Corporation's reasonable satisfaction, that it:

(A) can operate in a test environment, including, but not limited to, sending and receiving messages and transactions;

(B) can replay or resubmit previously submitted messages or transactions;

(C) can reverse or void previously submitted messages or transactions;

(D) can confirm the integrity of messages and transactions;

(E) has alternative communication methods with the Corporation to facilitate the exchange of messages, transactions, and reports; and

(F) can complete any other such requirements as are reasonably requested by the Corporation.

(2) Reconnection of a Clearing Member must be approved by two or more Designated Officers of the Corporation, in their reasonable judgement, after (i) the Corporation has received all required information pursuant to this Rule, in a form and substance satisfactory to the Corporation, and (ii) the requirements of Rule 213(h)(1) have been satisfied, as applicable.

(i) Certain Miscellaneous Matters.

(1) Without limiting any other provisions in these Rules concerning limitations on liability, neither the Corporation nor its directors, officers, employees, agents, or contractors shall be liable to any Clearing Member or any customer or client thereof for:

(A) any failure, hindrance, interruption or delay in performance in whole or in part of the obligations of the Corporation under these Rules, if that failure, hindrance, interruption or delay arises out of or relates to a Clearing Member System Event, Major Clearing Member System Event, or any action or inaction pursuant to this Rule 213; or

(B) any loss, liability, damage, cost or expense arising from or relating in any way to any advice, request, requirement, instruction, action or inaction pursuant to this Rule 213.

(2) The power of the Corporation to take any action pursuant to this Rule 213, or to request or require any action, documentation, or information pursuant to this Rule 213, also includes the power to

waive, repeal, rescind, revoke, amend, or vary any such action, request, or requirement in consideration of the facts and circumstances.

(3) The powers of the Corporation pursuant to this Rule 213 are in addition to, and not in limitation of, any authority granted elsewhere in these Rules to act as specified therein.

(4) All information related to or regarding a Major Clearing Member System Event and all acts pursuant to this Rule 213 will be considered Confidential Information pursuant to these Rules; provided, however, that the Corporation may inform, or direct the Clearing Member to inform, the Clearing Member's Third-Party Service Provider of a Clearing Member System Event if the Corporation determines, in its discretion, that such action is necessary for the protection of the Corporation and other Clearing Members.

(5) Failure of a Clearing Member to comply with the requirements of this Rule 213 may subject the Clearing Member to any and all disciplinary action permitted under these Rules, including, without limitation, suspension.

(6) A Clearing Member that has authorized another party, such as a Third-Party Service Provider, to access and use the Corporation's Systems will be responsible for such authorized party's compliance with the requirements of this Rule 213 and any compliance failure by that authorized party will be deemed to be a failure of the authorizing Clearing Member.