THE FOUNDATION FOR SECURE MARKETS®

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

June 5, 2023

By Electronic Submission

Vanessa Countryman, Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: RIN 3235-AN15 Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents

Dear Ms. Countryman:

The Options Clearing Corporation ("OCC") welcomes the opportunity to comment on the Securities and Exchange Commission's (the "SEC" or the "Commission") proposed rulemaking regarding cybersecurity risk management (the "Proposal" or "Rule 10").[1]

Founded in 1973, OCC is the world's largest equity derivatives clearing organization. OCC operates under the jurisdiction of both the SEC and the Commodity Futures Trading Commission (the "CFTC"). As a registered clearing agency under the SEC's jurisdiction, OCC clears and settles transactions for exchange-listed options. OCC is subject to Regulation Systems Compliance and Integrity ("Regulation SCI") under the Securities and Exchange Act of 1934. As a registered derivatives clearing organization under the CFTC's jurisdiction, OCC clears and settles transactions in futures and options on futures. OCC also provides central counterparty clearing and settlement services for securities lending transactions. In addition, OCC has been designated by the Financial Stability Oversight Council as a systemically important financial market utility ("SIFMU") under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act. As a SIFMU, OCC is subject to prudential regulation by the Board of Governors of the Federal Reserve System. OCC is recognized by the European Securities and Markets Authority as a Tier 1 CCP established in third countries under Article 25 of the European Market Infrastructure Regulation. OCC operates as a market utility and is owned by five exchanges.

[1] Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents, Release No. 34–97142, 88 Fed. Reg. 20212 (proposed Apr. 5, 2023) ("Release").

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

Summary and Overall Comments

OCC supports and appreciates the Commission enhancing its regulations to identify and protect the U.S. securities markets from cybersecurity vulnerabilities and threats, and generally to improve cybersecurity risk management across the industry. We agree that, as mentioned in the Proposal, the U.S. securities markets depend on Market Entities[2] to perform various functions without disruption to ensure market stability and operations, and that the interconnectedness of Market Entities potentially increases the risk of a cybersecurity incident impacting multiple entities for U.S. securities markets, which could result in considerable harm to the securities markets.[3] We further agree that the fair, orderly and efficient operations of all U.S. securities markets relies on the use of information systems and a network of interconnected information systems. OCC, like other clearing agencies, uses information systems to perform a variety of functions, including its core clearing and settlement functions, and relies on its interconnectedness with its participant exchanges and clearing members through networking and other system access to perform its self-regulatory organization obligations. OCC appreciates the Commission's efforts to strengthen the operational resilience of the securities markets through this Proposal.

The Commission is proposing that Covered Entities[4] adopt enhanced policies and procedures to identify, assess and respond to cybersecurity incidents[5] and mitigate cybersecurity risk. OCC recognizes that requiring consistent cybersecurity practices for all securities market participants will strengthen the cybersecurity of the securities marketplace and result in fewer cybersecurity incidents. While supportive of the principles of the Proposal, OCC respectfully requests that the Commission consider revising the Proposal to specify that Covered Entities may achieve compliance through the establishment and maintenance of policies and procedures that align

---

[2] Market Entity means: ""covered entity" as defined in [proposed Rule 10] and a broker or dealer registered with the Commission that is not a "covered entity" as defined in [proposed Rule 10]." Release at 20344. Covered entity, in turn, means: (i) A broker or dealer registered with the Commission that: (A) Maintains custody of cash and securities for customers or other brokers or dealers and is not exempt from the requirements of § 240.15c3-3; (B) Introduces customer accounts on a fully disclosed basis to another broker or dealer described in paragraph (a)(1)(i)(A) of this section; (C) Has regulatory capital equal to or exceeding $50 million; (D) Has total assets equal to or exceeding $1 billion;(E) Is a market maker under the Securities Exchange Act of 1934 (15 U.S.C. 78a, et seq.) ("Act") or the rules thereunder (which includes a broker or dealer that operates pursuant to § 240.15c3-1(a)(6)) or is a market maker under the rules of a self-regulatory organization of which the broker or dealer is a member; or (F) operates an alternative trading system as defined in § 242.300(a) or operates an NMS Stock ATS as defined in § 242.300(k). (ii) A clearing agency (registered or exempt) under Section 3(a)(23)(A) of the Act. (iii) A major security-based swap participant registered pursuant to Section 15F(b) of the Act. (iv) The Municipal Securities Rulemaking Board. (v) A national securities association registered under Section 15A of the Act. (vi) A national securities exchange registered under Section 6 of the Act. (vii) A security-based swap data repository under Section 3(a)(75) of the Act. (viii) A security-based swap dealer registered pursuant to Section 15F(b) of the Act. (ix) A transfer agent as defined in Section 3(a)(25) of the Act that is registered or required to be registered with an appropriate regulatory agency as defined in Section 3(a)(34)(B) of the [Exchange] Act. . . . Release at 20343.

[3] *See* Release at 20226.

[4] *See* note 2, *supra*.

[5] *See* Release at 20344.

with industry standards, as it has done with other similar regulations.[6] This change would support the Commission's stated objective of promoting the use of best practices in policies and procedures across Covered Entities.

OCC also appreciates the Commission's goals related to notification and reporting of significant cybersecurity incidents,[7] including the objective to improve the Commission's ability to monitor and evaluate the effects of significant cybersecurity incidents.[8] Although OCC agrees with the Commission's objective, OCC respectfully requests that the Commission consider modifying the Proposal to include reasonable reporting timelines to align with overlapping Commission regulatory requirements in order to enable OCC and other Covered Entities to focus cybersecurity personnel's undivided attention and efforts on the eradication and containment of incidents as a first priority.

Finally, we believe that the Proposal's public disclosure requirements for cybersecurity risks would introduce new risks to Covered Entities with potentially severe negative consequences to the securities markets. We are concerned that a Covered Entity's public disclosure of such risks could provide information to threat actors that increases the opportunity for these parties to compromise the security and integrity of the Covered Entity. We therefore respectfully request that the Commission reconsider the requirement for public disclosure of these cybersecurity risks given the real possibility that this information may be used as a roadmap for threat actors to compromise the securities markets generally.

Detailed Comments

Please note that for ease of reference, detailed comments set forth below are presented in the order in which the relevant provisions are discussed in the Proposal.

242.10(a)(10) Significant cybersecurity incident

The proposed definition of a "significant cybersecurity incident" does not specify what constitutes a "significant" incident. As proposed, a significant cybersecurity incident means:

> a cybersecurity incident, or a group of related cybersecurity incidents, that (i) Significantly disrupts or degrades the ability of the market entity to maintain critical operations; or (ii) Leads to the unauthorized access or use of the information or information systems of the market entity, where the unauthorized access or use of such information or information systems results in or is reasonably likely to result in: (A) Substantial harm to the market

[6] *See, e.g.,* 17 CFR 242.1001(a)(4) (stating that policies and procedures of SCI entities shall be deemed to be reasonably designed if they are consistent with current SCI industry standards).
[7] *See* Release at 20344-45.
[8] *See* Release at 20275.

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

entity; or (B) Substantial harm to a customer, counterparty, member, registrant, or user of the market entity, or to any other person that interacts with the market entity.[9]

OCC is concerned that the Proposal's language does not provide sufficient guidance for Covered Entities to develop a systematic approach to correctly classifying incidents as "significant." In the absence of objective standards for certain terms (e.g., "significantly," "critical," substantial," "reasonably likely"), the proposed definition of "significant cybersecurity incident" could lead to inconsistent application of the regulation both within and across Covered Entities. Without objective criteria, the determination of whether a significant cybersecurity incident is reasonably likely to occur will be left to each Covered Entity's cybersecurity professional's interpretation and analysis in light of the Covered Entity's particular risk profile, appetite, and cybersecurity posture. As a result, the Commission is likely to receive inconsistent reporting across Covered Entities which undermines its stated objective to monitor and evaluate cybersecurity incidents in aggregate across the marketplace.

OCC agrees with the Commission's objective to improve the Commission's ability to monitor and evaluate the effects of significant cybersecurity incidents and agrees that cybersecurity incidents of a certain severity and impact should be reported to the Commission. OCC requests that the Commission revise the proposed definition of a "significant cybersecurity incident" to include objective criteria further distinguishing a significant cybersecurity incident from a cybersecurity incident[10] to cultivate repeatable processes, promote consistent categorization of incidents across market participants, and support the objective of shared responsibility and consistency in cybersecurity standards and protocols.

242.10(b)(1) Cybersecurity policies and procedures

The Proposal would require that Covered Entities establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks. OCC supports the goal of the requirement and agrees that policies and procedures that address cybersecurity risks can identify and minimize cybersecurity risks and cultivate enhanced cybersecurity risk management across the securities markets. In the Proposal, the Commission notes that the policy and procedure requirements are not meant to impose a one-size-fits-all approach. OCC submits that the Proposal would be improved by including language permitting each Covered Entity to comply with Rule 10[11] by designing its procedures in conformance with industry standards much like what is permitted under existing Regulation SCI, which states that policies and procedures "shall be deemed to be reasonably designed if they are consistent with current SCI industry

[9] Release at 20344.
[10] "Cybersecurity incident" means "an unauthorized occurrence on or conducted through a market entity's information systems that jeopardizes the confidentiality, integrity, or availability of the information systems or any information residing on those systems." Release at 20343.
[11] Release at 20344.

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

standards."[12] OCC urges the Commission to consider mirroring the approach taken in Regulation SCI. By conforming policies and procedures to industry standards, Covered Entities would be required to update and modify policies and procedures as cybersecurity risks evolve and best practices progress.[13] We believe this approach conforms with the Commission's stated goal to not impose a "one-size-fits-all" approach but rather apply a flexible approach that can adapt to a changing cybersecurity landscape tailored to each Covered Entity's business needs. Therefore, OCC respectfully requests that the Commission confirm that consistency with industry standards will meet the "reasonably designed" standard for policies and procedures required by the Proposal.

242.10(b)(1)(iii)(B) Information Protection

OCC is generally supportive of the proposed information protection provisions as applied to Covered Entities and specifically supports the requirement for industry participants to create and maintain specific policies and procedures on cybersecurity risks. That said, in OCC's view, it appears that proposed Rule 10(b)(1)(iii)(B) would require Covered Entities to obtain from all service providers that "receive, maintain, or process" the Covered Entity's information, or who are "permitted to access the Covered Entity's information systems",[14] contractual promises that essentially treat these service providers as if the service providers themselves are Covered Entities under the Proposal. OCC believes that the Proposal's apparent requirement to contractually obligate service providers to comply with cybersecurity measures equivalent to proposed Rule 10[15] would pose an undue burden on Covered Entities while creating potentially significant disincentives for critical service providers to service the U.S. securities markets. As drafted, the Proposal would impose regulatory obligations on service providers that may be unable or unwilling to maintain the costly and stringent cybersecurity protocols outlined in the Proposal. As a result, OCC is concerned that the Proposal could limit the population of service providers willing and able to do business with

[12] 17 CFR 242.1001(a)(4).

[13] *See* Release at 20239 ("The policies and procedures that would be required by proposed Rule 10—because they would need to address the Covered Entity's cybersecurity risks—generally should be tailored to the nature and scope of the Covered Entity's business and address the Covered Entity's specific cybersecurity risks. Thus, proposed Rule 10 is not intended to impose a one-size-fits-all approach to addressing cybersecurity risks. In addition, cybersecurity threats are constantly evolving and measures to address those threats continue to evolve. Therefore, proposed Rule 10 is designed to provide Covered Entities with the flexibility to update and modify their policies and procedures as needed so that that they continue to be reasonably designed to address the Covered Entity's cybersecurity risks over time.")

[14] The Proposal defines "information" as "any records or data related to the Market Entity's business residing on the Market Entity's information systems." Release at 20343. The Proposal defines "information systems" as information resources that are owned or used by the Market Entity "for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the Covered Entity's information to maintain or support the Covered Entity's operations." Release at 20344.

[15] *See* id. The Proposal as drafted would require oversight of service providers that receive, maintain, or process the covered entity's information, or are otherwise permitted to access the covered entity's information systems and the information residing on those systems, pursuant to a written contract between the covered entity and the service provider, through which the service providers are required to implement and maintain appropriate measures, including the practices described in proposed Rules 10(b)(1)(i)-(v), that are designed to protect the covered entity's information systems and information residing on those systems.

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

Covered Entities – even for non-critical services. This limited population will likely result in concentration risk for access to certain services within the securities markets. OCC recommends the Commission limit the application of these provisions to those service providers that provide services to the Covered Entity that are critical for the maintenance of fair and orderly markets. This would limit the increased oversight and management burden to the high-risk service providers that may compromise the fair and orderly operation of the securities markets without adding unnecessary administrative obligations for low-risk activities.

242.10(c)(1) Immediate Notice

The Commission proposes requiring Covered Entities to immediately notify the Commission upon having a reasonable basis to conclude that a significant cybersecurity incident has occurred. OCC agrees in principle with the Commission that timely reporting of significant cybersecurity incidents can assist the industry in identifying and mitigating the occurrence of cybersecurity incidents throughout the securities markets and allow for the Commission to improve monitoring activity across the industry.

Unfortunately, in our view, the Proposal does not adequately weigh the burden that the Proposal would impose on Covered Entities also covered by Regulation SCI against the benefits the Proposal secures. Specifically, there is potential overlap with incident reporting for Covered Entities that are subject to both Regulation SCI and proposed Rule 10. In the Proposal, the Commission addresses the possibility of overlap by asserting that Regulation SCI and proposed Rule 10 reporting serve different purposes.[16] While we agree in theory that the reports required under Regulation SCI and proposed Rule 10 serve different purposes, in practical terms, the Covered Entity will likely need to submit multiple reports on the same matter under different timelines and different reporting criteria, thus creating potentially overlapping reports and reporting burdens on the Covered Entity. We believe that these layered reporting obligations are more likely to undermine the Commission's understanding of the cybersecurity threat landscape for the securities markets than enhance the Commission's understanding by requiring the Commission to decipher separate, technically nuanced responses from each report. In addition, these overlapping reporting requirements could strain a Covered Entity's incident response efforts as it requires the Covered Entity to simultaneously handle SEC reporting and respond to inquiries, detracting from optimal threat management.[17] The initial stages of an incident response require "all-hands-on-deck" to focus immediately and fully on understanding the incident and implementing mitigation and response measures. While the Commission purports to "provide the Covered Entity time to gather the information" elicited by Part I of proposed Form SCIR, a 48-hour reporting period would not likely yield the useful disclosure the

[16] *See* Release at 20275 ("Consequently, a Covered Entity that is also an SCI entity that experiences a significant cybersecurity incident under proposed Rule 10 that also is an SCI event would be required to make two filings for the single incident: one on Part I of proposed Form SCIR and the other on Form SCI. The Covered Entity also would be required to make additional filings on Forms SCIR and SCI pertaining to the significant cybersecurity incident (i.e., to provide updates and final reports)."

[17] The Commission envisions "engaging in discussions with the Covered Entity to understand better what steps it is taking to protect its customers, counterparties, members, registrants, or users. Release at 20249.

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

Commission seeks to secure due to an insufficient amount of time for a Covered Entity to fully understand the nature of the incident. It would instead require Covered Entities to divert time and resources away from effective incident response, potentially compromising the fair and orderly operation of the securities markets. As drafted, the Proposal would require the cybersecurity professionals employed by Covered Entities experiencing a significant cybersecurity incident to be subject to additional reporting responsibility at the same time their organization is most vulnerable to a cybersecurity threat, rather than directing their sole attention and efforts to the eradication of the threat actors and containment of the incident. OCC respectfully requests allowing Covered Entities time to assess significant cybersecurity risks and provide the Commission with the required information under detailed reporting obligations once a cybersecurity threat is contained, no later than 72 hours from having a reasonable basis to conclude that a significant cybersecurity incident has occurred.

242.10(d)Disclosure of cybersecurity risks and incidents

The Proposal would require Covered Entities to make two types of public disclosures: (i) a summary of the Covered Entity's cybersecurity risks[18] and (ii) significant cybersecurity incidents detected by the Covered Entity.[19] OCC agrees with the intent of this aspect of the Proposal; however, OCC disagrees that the stated goal of the Commission will be achieved by the Proposal as drafted.

"Cybersecurity risks" are defined as "financial, operational, legal, reputational, and other adverse consequences that could result from cybersecurity incidents, cybersecurity threats, and cybersecurity vulnerabilities."[20] This definition is intentionally broad[21] and was meant to capture all possible risks that could arise from cybersecurity threats and incidents. Disclosure of all cybersecurity risks would provide threat actors a roadmap that may provide information for future attacks, a feedback loop for current and past attacks, and a public scorecard demonstrating how cybersecurity is handled across each Covered Entity. As proposed, this requirement would require public disclosure of *how* the Covered Entity assesses, prioritizes, and addresses cybersecurity risks. Additionally, requiring a Covered Entity to indicate whether a cybersecurity incident has been remediated or is currently being remediated would further expose Covered Entities' cybersecurity vulnerabilities by highlighting the very systems that might not be fully operational due to the initial attacks, thereby increasing potential threats and compounding the likelihood of attacks from third parties. This type of information provides threat actors clues that they could use to carefully plan their next attack using the Covered Entity's cybersecurity risks and potentially known cybersecurity vulnerabilities that would be required to be publicly disclosed under the Proposal.

[18] *See* Release at 20345.
[19] *See id*.
[20] Release at 20343.
[21] *See* Release at 20232.

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

We request that the Commission reconsider the requirement to publicly disclose cybersecurity risks based on the sensitivity and potential for misuse of this information. The Commission should instead limit what may be publicly disclosed to best protect Covered Entities and the operation of fair and orderly securities markets. We understand why sharing this information *with the Commission* would be helpful to the Commission in supporting their oversight function; however, we disagree that public disclosure is necessary or appropriate. OCC respectfully requests that the Commission revise this requirement to allow Covered Entities to produce periodic, confidential reporting to the Commission. This would allow the Commission to achieve its stated goal of oversight and monitoring of cybersecurity risks and reduce the likelihood that significant cybersecurity incidents for a Covered Entity will have a ripple effect throughout the securities markets.

******

OCC thanks the Commission for the opportunity to comment on the Proposal and we look forward to a continued dialogue on the topic. Should you have any comments or questions regarding this submission, please contact Rebecca Riegert, Associate General Counsel, by telephone at (312) 322-1914 or by email rriegert@theocc.com.

Sincerely,

Megan Malone Cohen

Megan Malone Cohen
General Counsel and Corporate Secretary