June 5, 2023

Via Electronic Submission to rule-comment@sec.com

Ms. Vanessa A. Countryman, Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: 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, File No. S7-06-23

Dear Ms. Countryman:

Cboe Global Markets, Inc. ("Cboe") appreciates the opportunity to comment on the proposal of the Securities and Exchange Commission ("SEC" or "Commission") in the above-referenced file number (the "Proposal").

Cboe is a global operator of financial markets, including six national securities exchanges[1] and an Alternative Trading System ("ATS").[2] Our focus as a global markets operator is to provide trusted, liquid, and resilient markets in support of a larger ecosystem that serves and benefits all investors.

Cboe is committed to cybersecurity risk management and supports requirements to establish, maintain, and enforce written policies and procedures that are reasonably designed to address cybersecurity risks and periodically review their effectiveness. In this regard, Cboe has developed, implemented, and maintains a robust Information Security and Privacy Program in all of its regulated market venues, including policies, procedures, and safeguards to offset possible threats and delineate operational accountability. We consider our Information Security and Privacy Program essential to protecting the confidentiality, integrity, and availability of information assets,

---

[1] Cboe operates six national securities exchanges in the United States: Cboe Exchange, Cboe C2 Exchange, Cboe BYX Exchange, Cboe BZX Exchange, Cboe EDGA Exchange, and Cboe EDGX Exchange.

[2] Cboe owns BIDS Trading, which operates as an ATS. BIDS Trading is not a national securities exchange or a facility thereof.

including personal data, and mitigating the likelihood, frequency, and severity of information security incidents and system disruptions and malfunctions.

It is this commitment to cybersecurity risk management that has resulted in Cboe's extensive cybersecurity program and protections, prior to and outside of any specific regulatory requirements. The marketplace demands it. Cboe's users demand it. In addition, numerous other federal, state, and foreign laws and regulations demand it.

As such, Cboe supports efforts to related to policies and procedures to address cybersecurity risks. However, Cboe recommends changes to the Proposal for better alignment and consistency with existing cybersecurity frameworks. Doing so will assist in fostering resilience through the prevention and mitigation of cyberattacks, while at the same time reducing unnecessary risk as well as compliance burdens and costs.

"Cybersecurity Incident"

Cboe recommends that the Commission amend the proposed definition of "Cybersecurity Incident" or otherwise clarify that an unsuccessful attempt to obtain unauthorized access to, or to interfere with the operations of, a Covered Entity's systems would not be considered a "unauthorized occurrence." Under proposed Rule 10(a)(2), a "Cybersecurity Incident" is defined as "… 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." The proposed definition does not expressly include unsuccessful attempts, but we are concerned that the term "unauthorized occurrence" could be read to include an unsuccessful attempt. If an attempt is unsuccessful, it means that the covered entity prevented the intended harm. In our view, requiring written documentation of every unsuccessful attack would unnecessarily distract from focusing on any cybersecurity incidents that do have impact.

"Significant Cybersecurity Incident"

Cboe recommends that the Commission amend the definition of "Significant Cybersecurity Incident" to "Material Cybersecurity Incident." Amending the definition this way would be consistent with previous Commission determinations discussed below, and it would result in disclosure to the Commission that is tailored to the particular facts and circumstances of each Covered Entity. Amending to the term to "Material Cybersecurity Incident" would achieve greater consistency, not only with other rulemaking, but within the Proposal itself. For example, as noted in the Proposal, a Covered Entity (such as a national securities exchange or an ATS) would be required to make disclosures relating to cybersecurity on proposed Form SCIR.[3] The Covered Entity "would need to, in plain English, provide a summary description of the cybersecurity risks that could ***materially*** affect its business and operations and how the Covered Entity assesses, prioritizes, and addresses those cybersecurity risks."[4] (Emphasis added.) As mentioned in the Proposal, cybersecurity risk would be material to a Covered Entity if there is a substantial

---

[3] *See* paragraph (d)(1) of proposed Rule 10.

[4] *See* paragraph (d)(1)(i) of proposed Rule 10; Line Item 2 of Part II proposed of Form SCIR.

likelihood that a reasonable person would consider the information important based on the total mix of facts and information.[5] Accordingly, the word "material" should be used in lieu of "significant" in the Proposal definitions.

We note that the 2022 proposed rule entitled "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" (the "2022 Proposal") also uses the term "material." Specifically, in the 2022 Proposal, the Commission set forth amendments "to require current reporting about ***material*** cybersecurity incidents,"[6] with the intended purpose "to better inform investors about a registrant's risk management, strategy, and governance and to provide timely notification of ***material*** cybersecurity incidents."[7] (Emphasis added). The 2022 Proposal is intended to reflect the policy goal of benefiting investors from more timely and consistent disclosure about ***material*** cybersecurity incidents, because of the potential impact that such incidents can have on the financial performance or position of a registrant.[8] Additionally, the 2022 Proposal references Commission-issued interpretive guidance, recognizing the need for investors to be informed about ***material*** cybersecurity risks and incidents in a timely manner and to assist operating companies in determining when they may be required to disclose information regarding cybersecurity risks and incidents under existing disclosure rules.[9] For all Covered Entities, including national securities exchanges and ATSs, the use of the use of the term "material" instead of "significant" in the Proposal definitions would create consistency and alignment with previous policy determinations and other rulemaking.

The materiality approach also would be consistent with the Commission's approach to risk disclosure in registration statements. Since the Commission first published guidance on risk factor disclosure in 1964,[10] it has underscored that risk factor disclosure should be focused on the "most significant" or "principal" factors that make a registrant's securities speculative or risky.[11] Notwithstanding that guidance, the length of risk factor disclosure and the number of risks disclosed increased in subsequent years. As a result, the Commission made amendments to change the standard for disclosure from the "most significant" risks to "material" risks[12] to focus

---

5 *S.E.C. v. Steadman*, 967 F.2d 636, 643 (D.C. Cir. 1992); cf. *Basic Inc. v. Levinson*, 485 U.S. 224, 231-232 (1988); *TSC Industries v. Northway, Inc.*, 426 U.S. 438, 445, 449 (1976).

6 *See* Summary for Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, [Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22]

7 *Id.*

8 Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, [Release Nos. 33-11038; 34-94382; IC-34529; File No. S7-09-22], page 11.

9 *See* Commission Statement and Guidance on Public Company Cybersecurity Disclosures, Release No. 33-10459 (Feb. 26, 2018) No. 33-10459 (Feb. 21, 2018) [83 FR 8166], *available at* https://www.sec.gov/rules/interp/2018/33-10459.pdf.

10 *See* Guides for Preparation and Filing of Registration Statements, Release No. 33-4666 (Feb. 7, 1964) [29 FR 2490 (Feb. 15, 1964)] ("1964 Guides").

11 "Principal" was the term used in the 1982 Integrated Disclosure Adopting Release and "most significant" was the term used in the Plain English Disclosure Adopting Release.

12 Securities Act Rule 405 [17 CFR 230.405] and Exchange Act Rule 12b-2 [17 CFR 240. 12b-2] both generally define materiality as information to which there is a substantial likelihood that a reasonable investor would

registrants on disclosing the risks to which reasonable investors would attach importance in making investment or voting decisions.

Notification and Reporting

Cboe recommends that the Commission modify the proposed requirement to provide "immediate" written notice of a Significant Cybersecurity Incident and allow Covered Entities to make the required notifications orally. As proposed, the requirement would force a Covered Entity that has just discovered and begun dealing with a cybersecurity attack to notify the Commission in writing before addressing the incident itself.[13] The Proposal requires (emphasis added) that "[a] covered entity must give the Commission ***immediate written electronic notice*** of a significant cybersecurity incident upon having a reasonable basis to conclude that the significant cybersecurity incident has occurred ***or is occurring***." The notification requirement could add distraction and delay to an already intense process by demanding immediate attention from management to satisfy this requirement during the most critical initial period of identifying and responding to an incident.

We believe that the Commission's priority should be to provide information and assistance to support cybersecurity efforts, and, following resolution, to collect information that will provide future benefits. The requirement to provide immediate notice in writing creates the potential for greater legal and compliance risk for an entity experiencing a cybersecurity incident, a risk that will cause diversion from fully focusing energies on identifying and mitigating the immediate threat to navigating aggressive deadlines and information requirements of the Commission. In addition, we note that the Commission permits oral notification of SCI events.[14]

While we do not support the requirement for immediate written notice, we agree that cybersecurity is a topic of utmost importance and the potential for harm to the economy, markets, market participants, and investors is significant. We remind the Commission that in March 2022, President Biden signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Enactment of CIRCIA was intended to improve "America's cybersecurity by, among other things, requiring the Cybersecurity and Infrastructure Security Agency (CISA) to develop and implement regulations requiring covered entities to report to CISA covered cyber incidents and ransom payments. This is to allow CISA to rapidly deploy resources and render assistance to victims suffering attacks, analyze incoming reporting across sectors to spot trends, and quickly share that information with network defenders to warn other potential victims."[15] As the Commission may already be aware, CIRCIA does not have an "immediate notice" requirement,

---

attach importance in its investment decision. See also Modernization of Regulation S-K Items 101, 103, and 105 [17 CFR 229, 239, and 240], adopting the amendment as proposed to "change the standard for disclosure from the 'most significant' risks to 'material' risks to focus registrants on disclosing the risks to which reasonable investors would attach importance in making investment or voting decisions."

13 Additionally, covered entities would also be required to file Part I of new Form SCIR confidentially on EDGAR within 48 hours, which would contain detailed information about the incident and would need to be continually updated if additional material developments occur.

14 *See* "Division of Trading and Markets: Responses to Frequently Asked Questions Concerning Regulation SCI" (September 2, 2015; Updated August 21, 2019), Response to Question 3.02.

15 https://www.cisa.gov/sites/default/files/publications/CIRCIA_07.21.2022_Factsheet_FINAL_508%20c.pdf

rather the provisions of CIRCIA require covered entities to provide notification of any covered cyber incidents within 72 hours.[16] Even payments for ransomware require 24 hours' notice,[17] not "immediate notice"(written or otherwise).

Reasonable Basis to Conclude that the Significant Cybersecurity Incident…or is Occurring

Under the Proposal, a Covered Entity would be required to give the Commission immediate written electronic notice of a Significant Cybersecurity Incident upon having a ***reasonable basis*** to conclude that the Significant Cybersecurity Incident has occurred ***or is occurring***. It is often difficult to immediately discern between an incident requiring a disaster recovery response and a cybersecurity incident. Both require the process of information technology teams trying to get technology back up and running, but the determination that such an incident is in fact a cybersecurity incident may not be immediately or readily apparent. As such, the notice requirement should be triggered with the Covered Entity has an "actual basis" that the incident "has occurred." The proposed rules would impose substantial regulatory obligations in the event of a Significant Cybersecurity Event, and those obligations could create unnecessary burdens on Covered Entity that had to fulfill those obligations for an incident that ultimately was not subject to the requirements of Rule 10. In addition, we note that Regulation SCI requires immediate notice by SCI entities when there is a "reasonable basis to conclude that an SCI event **has occurred**."[18]

Public Disclosure

Cboe recommends that the Commission remove the proposed requirement for public disclosure of Cybersecurity Incidents. Proposed Rule 10 would require public disclosure of the following information, to the extent known, for any Significant Cybersecurity Incident:

(A) The person or persons affected;
(B) The date the incident was discovered and whether it is ongoing;
(C) Whether any data was stolen, altered, or accessed or used for any other unauthorized purpose;
(D) The effect of the incident on the Covered Entity's operations; and
(E) Whether the Covered Entity, or service provider, has remediated or is currently remediating the incident.

Cboe is opposed to this public disclosure requirement for at least two reasons. First, this disclosure, in many cases, could provide valuable information to malicious third-party actors that seek to obtain unauthorized access to, or interfere with the operations of, a Covered Entity's systems. Second, the requirement for public disclosure presents the risk that the failure of a Covered Entity to provide a public disclosure would signify to attackers that the Covered Entity is not aware of an

---

16 *See* Cyber Incident Reporting for Critical Infrastructure Act of 2022, March 9, 2022: Publication, SEC 2242. Required Reporting of Certain Cyber Incidents §(a)(1)(B) *available at* https:// www.cisa.gov/resources-tools/resources/cyber-incident-reproting-critical-infrastructure-act-2022-publication

17 *Id at* SEC 2242. Required Reporting of Certain Cyber Incidents §(a)(2)(A)

18 Rule 1002(b)(1) of Regulation SCI under the Exchange Act.

attack. The potential negative impact of any such public disclosure significantly outweighs any potential benefit.

In addition, Cboe disagrees with any requirement to publicly identify specific persons that have been affected by a Significant Cybersecurity Incident. Any affected persons should be notified directly by the Covered Entity and should not be identified in a public disclosure. The proposed Rule 10 would require a Covered Entity to provide, through a mandated public disclosure on Part II of the proposed Form SCIR, "… a summary description of each significant cybersecurity incident that has occurred during the current or previous calendar year." This summary description must include, to the extent known, "… the person or persons affected." This disclosure is potentially inconsistent with federal and state privacy laws, the privacy laws of other countries, and confidentiality agreements and obligations to which a Covered Entity is subject.

If the Commission decides to adopt a public disclosure requirement, Cboe recommends that the rule include an express exception that would allow a Covered Entity to exclude from any public disclosure any incident (or any information relating to an incident) where the Covered Entity reasonably determines that the public disclosure of such incident or information: (1) could assist a malicious third-party actor in obtaining unauthorized access to, or interfering with the operations of, the Covered Entity's systems (or the systems of another entity); or (2) would be inconsistent with applicable federal, state, or foreign law.

Scope

The Commission should clarify that the Proposal does not apply to exchanges that are notice-registered with the Commission pursuant to Section 6(g) of the Securities Exchange Act of 1934, as amended ("Act"). The Proposal appears to contemplate that notice-registered security futures exchanges are not covered by the Proposal since the Proposal does not list Cboe Futures Exchange, LLC (a notice-registered security futures exchange) as one of the national securities exchanges currently registered with the Commission that would meet the definition of a Covered Entity under Rule 10(a)(1).[19]

However, the Commission should make clear that this is the case by specifically providing in the definition of a Covered Entity in Rule 10(a)(1)(vi) that notice-registered security futures exchanges are not within the scope of Rule 10. The definition in Proposed Rule 10(a)(1)(vi) is overly broad because it applies to a national securities exchange registered under Section 6 of the Act and since Section 6(g) of the Act includes the provision for the notice-registration of notice-registered security futures exchanges with the Commission.

The Commission recognized in the adopting release for Regulation Systems Compliance and Integrity ("Regulation SCI") that notice-registered security futures exchanges are subject to the primary oversight of the Commodity Futures Trading Commission ("CFTC") and thus should not be subject to systems integrity regulations like the Proposal:

---

[19] *See* text preceding footnote 746 of the Proposal and the text preceding and included in footnote 946 of the Proposal.

> The Commission notes that such entities are subject to the joint jurisdiction of the Commission and the CFTC. To avoid duplicative regulation, however, the [Commodity Futures Modernization Act of 2000 ("CFMA")] established a system of notice registration under which trading facilities and intermediaries that are already registered with either the Commission or the CFTC may register with the other agency on an expedited basis for the limited purpose of trading security futures products. A "notice registrant" is then subject to primary oversight by one agency, and is exempted under the CFMA from all but certain specified provisions of the laws administered by the other agency. *See* Section 6(g)(4) and Section 15A(k)(3)-(4) (enumerating the provisions of the Exchange Act from which a notice-registered exchange and limited purpose national securities association, respectively, are exempted). Given this, the Commission believes that it is appropriate to defer to the CFTC regarding the systems integrity of these entities). (See 79 FR 72252, 72261, footnote 86.)

This approach is appropriate since notice-registered securities exchanges are subject to the comprehensive regulation and oversight of the CFTC, including being subject to the requirements of Core Principle 20 applicable to designated contract markets under Section 5(d)(20) of the Commodity Exchange Act and CFTC Regulation 38.1051, which both relate to system safeguards.

The Commission should adopt a similar approach to the one it took in the definitions within Regulation SCI, an approach which it has not proposed to alter in connection with its recent proposal to amend Regulation SCI. In particular, Regulation SCI explicitly excludes notice-registered security futures exchanges from the scope of Regulation SCI by making this exclusion clear in the definition of an SCI self-regulatory organization:

> SCI self-regulatory organization or SCI SRO means any national securities exchange, registered securities association, or registered clearing agency, or the Municipal Securities Rulemaking Board; provided however, that for purposes of this section, the term SCI self-regulatory organization ***shall not include an exchange that is notice registered with the Commission pursuant to 15 U.S.C. 78f(g)*** or a limited purpose national securities association registered with the Commission pursuant to 15 U.S.C. 78o-3(k). (Emphasis added) (7 C.F.R. 242.1000)

The Commission should include a similar exclusion to the one highlighted above in the definition of a Covered Entity under Rule 10(a)(1)(vi).[20]

****

Cboe appreciates the opportunity to comment on the Proposal from the Commission. We believe our recommendations would support the Commission's objectives to prevent and mitigate

---

[20] Although Cboe's focus in this regard is on notice-registered national securities exchanges given that CFE occupies that status, Cboe notes that the rationale for explicitly excluding notice-registered national securities exchanges from the scope of a Covered Entity under Rule 10 also applies to limited purpose national securities associations as it does in the context of Regulation SCI, and assumes that the exclusion would apply to any entity in that capacity as well.

cyberattacks, while at the same time reducing unnecessary risk as well as compliance burdens and costs. We welcome further discussions with the Commission

Sincerely,

/s/ Patrick Sexton

Patrick Sexton
EVP, General Counsel & Corporate Secretary

cc: The Honorable Gary Gensler, Chairman, SEC
The Honorable Caroline A. Crenshaw, Commissioner, SEC
The Honorable Hester M. Peirce, Commissioner, SEC
The Honorable Jaime Lizárraga, Commissioner, SEC
The Honorable Mark T. Uyeda, Commissioner, SEC
Director Haoxiang Zhu, Division of Trading and Markets