Hope M. Jarkowski
General Counsel
New York Stock Exchange
11 Wall Street
New York, NY 10005
T: 202.661.8946
Hope.Jarkowski@nyse.com

NYSE
AN ICE EXCHANGE

June 5, 2023

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

Re: File No. S7-06-23: 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:

Intercontinental Exchange, Inc. and its affiliates ("ICE") appreciates the opportunity to comment on the U.S. Securities and Exchange Commission's ("SEC" or the "Commission") proposed rule ("Proposal" or "Rule 10")[1] to require certain market entities to address cybersecurity risks through (i) the adoption of policies and procedures, (ii) incident reporting, and (iii) public disclosures. ICE is a leading provider of market infrastructure, data services and technology solutions to a broad range of customers including financial institutions, corporations, and government entities. We operate 13 regulated exchanges, six clearing houses, and two SEC-registered broker-dealers. Numerous ICE entities would be impacted by requirements contained in the Proposal.

ICE is generally supportive of the Commission's efforts to implement specific cybersecurity requirements for broker-dealers, clearing agencies, securities exchanges and swap data repositories. As an operator of global markets, ICE is keenly aware of the importance that robust cybersecurity policy has on its business and the protection of the financial services ecosystem. To that end, ICE has developed a comprehensive strategy to evaluate and manage our cybersecurity risk and believe that much of our existing approach is responsive to the Proposal's requirements.

With the benefit of our significant experience managing cybersecurity risk across our varied platforms, we offer the following comments on the Proposal for the Commission's consideration:

[1] https://www.sec.gov/rules/proposed/2023/34-97142.pdf

1. The Definition of "Cybersecurity Risk" is Overly Broad and Makes Compliance with Proposed Rule 10 Impractical.

Proposed Rule 10 is designed to ensure that designated Covered Entities[2] adequately address their cybersecurity risk. The Proposal requires the adoption of wide-ranging policies and procedures and mandates an ongoing reporting regime, in each case triggered by a Covered Entity's assessment of its "cybersecurity risk." The Proposal's definition of "cybersecurity risk" is so expansive, however, that compliance would be nearly impossible. Under the Proposal,

- "Cybersecurity risk" means financial, operational, legal, reputational, and other adverse consequences that could result from cybersecurity incidents, cybersecurity threats, and cybersecurity vulnerabilities.[3]

- "Cybersecurity threat" means any potential occurrence that may result in an unauthorized effort to affect adversely the confidentiality, integrity, or availability of a market entity's information systems or any information residing on those systems."[4]

Taken together, Covered Entities would need to develop policies to address--and publicly report on--the risk of *any potential* cybersecurity intrusion that *may* adversely impact *any of* their systems or information. The universe of such risks is practically infinite and, given the ever-changing tactics of bad actors, often unpredictable.

We urge the Commission to consider amending the proposed definitions of "cybersecurity risk" and "cybersecurity threat" to account for notions of materiality, reasonableness, and likelihood. Failure to qualify these definitions will result in policies and reporting that is either (i) so extensive that is becomes untethered from actual cybersecurity risk, or (ii) noncompliant with the plain language of proposed Rule 10.

2. Rule 10's Requirement for Real-time Reporting of Cybersecurity Incidents is Unnecessarily Burdensome and Will Impede the Ability to Effectively Respond to Critical Events.

Rule 10 requires Covered Entities to give the Commission "immediate written electronic notice of a significant cybersecurity incident upon having a *reasonable basis* to conclude that [such

---

[2] Under proposed Rule 10 a "Covered Entity" means "(i) a broker or dealer registered with the Commission [that meets specified requirements], (ii) a clearing agency (registered or exempt) under Section 3(a)(23)(A) of the Securities Exchange Act of 1934 (the "Act")…(iv) the Municipal Securities Rulemaking Board, (v) a national securities associated registered under section 15A of the Act, (vi) a national securities exchange registered under section 6 of the Act.."

[3] See Rule 10(a)(3).

[4] See Rule 10(a)(4).

incident] has occurred or is occurring."[5] Much like the comment above, the term "significant cybersecurity incident" is defined broadly. It is "a single cybersecurity incident or group of related cybersecurity incidents" that is, among other things, "*reasonably likely* to result in substantial harm to the market entity…, a customer, counterparty, member, registrant, or user of the market entity, or to *any other person that interacts with the market entity*."[6] Under the Proposal, reporting of such events is required to be made within 48 hours and continuously updated each time new material information is discovered.

Given the breadth of this reporting obligation, it is notable that Rule 10 offers no guidance as to what constitutes a "reasonable basis" or "reasonably likely." Even more troubling, the reporting requirement is triggered when "any person" that "interacts" with [a] market entity" is reasonably likely to suffer substantial harm from a cybersecurity incident, but Rule 10 does not define--or in any way explain--what it means to "interact" with a market entity. For market entities like the New York Stock Exchange, this could capture almost any individual who participates in the financial markets.

As stated in the Proposal, cybersecurity incidents are increasing in frequency and sophistication and can be carried out though a variety of different tactics by actors both known and unknown. Remaining vigilant against these acts is a full-time endeavor and Rule 10's burdensome reporting regime risks distracting market entities from undertaking this critical work. When a cybersecurity incident occurs, the primary focus of a market entity should be to thwart the attack and ensure the security of its systems as quickly as possible. Rule 10 diverts attention from this crucial response by saddling market entities with the obligation to assess whether "any person" who "interacts" with the market entity is "reasonably likely" to suffer harm from the incident. This extremely difficult assessment must be completed--and reported on--within 48 hours while an event may be ongoing and important facts yet unknown.

The burdens imposed by Rule 10 risk shifting the focus to reporting on, rather than responding to, a cybersecurity event. To forestall this undesirable result, ICE strongly recommends that the Commission (i) narrow the scope of the assessment to be undertaken by market entities by tailoring definitions contained in Rule 10, and (ii) extend the timeframe for submission of required reporting.

3. Required Disclosure of Cybersecurity Incidents on Form SCIR Imperils Covered Entities by Publicizing Sensitive Information.

Proposed Rule 10 would require Covered Entities to annually file Part II of new Form SCIR where they disclose a summary description of cybersecurity risks and detailed information about cybersecurity incidents that have occurred during the current or previous year. While general disclosures around cybersecurity risks and mitigation strategy may be beneficial to market participants, we believe that detailed disclosure about prior cybersecurity intrusions jeopardizes the market by exposing vulnerabilities that may be further exploited against the reporting entity

[5] See Rule 10(c).

[6] See Rule 10(a)(10)(ii)(B).

or others. Even if a cybersecurity intrusion is not ultimately successful, bad actors benefit from understanding how the intrusion impacted a victim's operation and whether it revealed weaknesses that remain unremediated. This sensitive material is precisely what is required to be publicly reported under Rule 10. Given that this same information would be submitted to the Commission under Part I of Form SCIR, thereby providing the Commission with the opportunity to evaluate the sufficiency of a Covered Entity's response to a cybersecurity event, we do not believe the benefit of public disclosure outweighs the risk that such information may be misused by cyber criminals seeking to inflict further harm. We urge the Commission to remove the public disclosure requirement of prior cybersecurity incidents from any final rule.

4. Required Oversight of Third-party Service Providers Is Unmanageable and Jeopardizes Covered Entities' Ability to Outsource.

Included among its sweeping policy and procedure requirements, proposed Rule 10 obligates Covered Entities to oversight "service providers that receive, maintain, or process the Covered Entity's information…"[7] Under this provision, Covered Entities must contractually bind these third-party service providers to "implement and maintain appropriate measures" related to, among other things, risk assessment, user access controls, and cybersecurity incident response. The Proposal offers general ideas for how a Covered Entity might conduct this challenging oversight, but is silent on the more problematic aspects of this requirement. In particular, the Proposal does not acknowledge the disputes that will inevitably arise when unrelated parties disagree on topics as nebulous as "vulnerability management" and the impact those disputes could have on the performance of critical contractual relationships.

ICE requests that the Commission remove this third-party oversight from any final rule. The requirements proposed by Rule 10 are already substantial. Adding them by compelling Covered Entities to manage the cybersecurity risk of their service providers--in addition to their own--will discourage the outsourcing of services that are more effectively performed by third parties than by a Covered Entity.

5. The Commission Should Coordinate with other Regulatory Agencies to Facilitate Efficient Compliance.

ICE notes that many SEC-Registered Clearing Agencies, including ICE Clear Credit and ICE Clear Europe, are also registered as Derivative Clearing Organizations ("DCO") with the Commodity Futures Trading Commission ("CFTC"). In addition, several security-based swap data repositories, including ICE Trade Vault, are also registered with the CFTC. The existing CFTC system safeguard regulations[8] as well as the CFTC Proposed Rulemaking relating to

---

[7] See Rule 10(b)(1)(iii)(B).

[8] System Safeguard Testing Requirements (RIN 3038–AE30), Federal Register 64272; Final Rule (September 19, 2016). See also System Safeguard Testing Requirements (RIN 3038-AE29), Federal Register 64321-64340 (September 19, 2016).

Reporting and Information Requirements for DCOs[9] overlap with the Proposal in many important ways. ICE urges coordination between the agencies to ensure that any final rules are structured so that dual-registered entities can efficiently comply with both agencies' rules.

Conclusion

We recognize the importance of cybersecurity risk management on the integrity of financial markets and commend the Commission for focusing attention on this critical subject. The comments provided herein are intended to help strike the appropriate balance between enhancing cybersecurity risk management on the one hand, while remaining mindful that onerous reporting and far-reaching rules may have the unintended effect of bolstering the behavior they seek to deter.

* * * *

Respectfully submitted,

Hope M. Jarkowski
General Counsel
NYSE Group, Inc.

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

[9] Reporting and Information Requirements for Derivatives Clearing Organizations (RIN 3038-AF12), 87 Fed. Reg. 76698 (Dec. 15, 2022).