ISDA Safe, Efficient Markets

June 5, 2023

Submitted Electronically

Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street N.E.
Washington, D.C. 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; RIN 3235-AN15]

Dear Ms. Countryman:

The International Swaps and Derivatives Association, Inc. ("**ISDA**")[1] appreciates the opportunity to submit these comments on the *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* ("**Proposed Rules**" or "**Proposal**") published by the U.S. Securities and Exchange Commission ("**SEC**" or "**Commission**") in the Federal Register on April 5, 2023.[2]

We agree with the Commission and the Financial Stability Oversight Counsel that cybersecurity risk has risen to the top of the list for financial institutions as it can lead to the loss of confidentiality, integrity, or availability of information, data, or control systems resulting in adverse consequences to a firm's operations.[3] Cybersecurity is a threat to the safe and efficient operation of financial markets, and thus, we are supportive of the Commission's efforts to ensure that market participants have robust policies and procedures in place, as well as the necessary tools, to avoid and quickly respond to cybersecurity threats and incidents.

[1] Since 1985, ISDA has worked to make the global derivatives markets safer and more efficient. Today, ISDA has more than 1,000 member institutions from 79 countries. These members comprise a broad range of derivatives market participants, including corporations, investment managers, government and supranational entities, insurance companies, energy and commodities firms, and international and regional banks. In addition to market participants, members also include key components of the derivatives market infrastructure, such as exchanges, intermediaries, clearing houses and depositories, as well as law firms, accounting firms and other service providers. Additional information on ISDA is available at http://www.isda.org.

[2] 88 Fed. Reg. 20212 (Apr. 5, 2023), *available at* https://www.govinfo.gov/content/pkg/FR-2023-04-05/pdf/2023-05767.pdf [hereinafter, Proposed Rules].

[3] Proposed Rules at 20213.

While we support the Commission's efforts to establish a regulatory framework for cybersecurity risk management, we are concerned that the Proposed Rules, in certain instances, are overly prescriptive, do not possess the necessary flexibility to allow firms to tailor their responses to the unique characteristics of a particular cybersecurity incident, and may superfluously overlap with the regulatory requirements of other domestic and foreign authorities.[4] When it comes to implementing a cybersecurity regulatory framework, it is essential that the financial industry speaks to the regulatory community in one voice. In this regard, we fully support the comments provided by the Securities Industry and Financial Markets Association ("**SIFMA**") in response to the Proposed Rules. Our response below reiterates SIFMA's concerns through highlighting five (5) key issues and provides recommendations for improvement that are particularly important to our collective membership.

1. The Timeframe for Cybersecurity Incident Reporting Should Be Aligned with Other Regulators' Requirements.

The Proposal's requirement that firms provide immediate written electronic notice to the SEC would negatively impact firms' ability to respond to significant cybersecurity incidents efficiently and effectively.[5] At the onset of a significant cybersecurity incident, a firm must have access to all of its resources so that it can focus on understanding the extent of the incident and assessing and coordinating the firm's response. Requiring "immediate" regulatory notice will only divert staff and resources towards fulfilling that obligation, rather than the firm-wide response to the incident—thereby interfering with the firm's ability to adequately respond to the incident and minimize the operational impacts of the cyber-attack.

In addition, as cybersecurity incidents are an industry-wide concern, the Commission should set out reasonable timelines that are in line with other regulators in order to allow firms to focus on resolving incidents, instead of meeting superficial deadlines that may divert from the key objective — providing accurate information to regulators that would enable them to assess the possible effects of a significant cybersecurity incident on financial markets. In this regard, reporting the same incident at different times to different regulators is not only burdensome and confusing, but may encourage cursory analysis that would defeat the Commission's key objective.

Moreover, the proposed timeframe of "immediate" notice is unreasonably shorter than the requirements of other regulators. For example, the National Futures Association issued an Interpretive Notice on Information Systems Security Programs which requires reporting of cyber incidents "promptly" (and not "immediately") after their occurrence.[6] This requirement is

[4] "Firm(s)" as used herein refer to those entities subject to the relevant Proposed Rule and defined as "Covered Entities" or "Market Entities" under the Proposed Rules. We are particularly concerned with the Proposed Rules' application to Security-Based Swap Dealers and Clearing Agencies as such entities form part of ISDA's membership.

[5] Proposed Rules at 20248.

[6] https://www.nfa.futures.org/rulebooksql/rules.aspx?RuleID=9070&Section=9

applicable to many entities that would be subject to the Proposal.[7] Also, the federal banking agencies take a more amenable approach that provides flexibility in manner of notification, as their rules require notification by phone or email and leave it up to the firm to determine the content of that notification.[8] Further, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("**CIRCIA**") provides for a 72-hour window to report a cybersecurity incident.[9] This is a more reasonable timeframe as it would allow firms to appropriately divert critical resources towards the incident instead of rushing to submit a vague and/or incomplete report in order to ensure compliance with the notification requirement. Unlike the Proposed Rules, each of these other approaches acknowledge the importance of flexibility and not unduly burdening firms with prescriptive notice requirements during the initial stages of a significant cybersecurity incident which is likely to be a high-pressure environment.[10]

For these reasons, ISDA recommends that the SEC adopt a more flexible approach when calibrating the notification window, similar to the approaches taken by the NFA, the banking agencies, and in CIRCIA. At a minimum, we ask the Commission to provide, at least, a 72-hour window for the regulatory notification of significant cybersecurity incidents. We believe the extended reporting timeline would better serve the SEC's stated goal to provide timely, accurate and meaningful information to market participants and enable them to assess possible effects of a significant cybersecurity incident.

2. The Premature Public Disclosure of Cyber Incidents May Encourage More Cyber Attacks.

The Commission's requirement that significant cybersecurity incidents must be disclosed through EDGAR and published on a firm's website could result in more harm to the firm, than it would benefit the general public, by potentially increasing the risk of cyber-attacks.[11] Publication of such incidents could result in vulnerabilities being exploited before the firm or its service

[7] Specifically, security-based swap dealers that are dually registered with the CFTC as swap dealers.
[8] The Office of the Comptroller of the Currency; the Board of Governors of the Federal Reserve System; and the Federal Deposit Insurance Corporation: Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66424 ("The final rule is designed to ensure that the appropriate agency receives timely notice of significant emergent incidents, while providing flexibility to the banking organization to determine the content of the notification. Such a limited notification requirement will alert the agencies to such incidents without unduly burdening banking organizations with detailed reporting requirements, especially when certain information may not yet be known to the banking organizations.").
[9] 6 U.S.C. § 681b(a)(1)(B) (providing that, although a covered entity shall report the covered cyber incident to CISA "not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred" the Director "may not require reporting . . . any earlier than 72 hours after the covered entity reasonably believes that a covered cyber incident has occurred.").
[10] The SEC also stated its goal through this requirement was to begin conversations with the relevant firm to ensure adequate customer and counterparty protection. Responding to government inquiries requires an extraordinary amount of resources and thus impedes firms' efforts to investigate and remediate the incident. This could compromise the firm's ability to best protect customers and counterparties if they must also engage in a dialogue with the Commission during the early stages of a cyber-response. Proposed Rules at 20248, 20249, 20256.
[11] Proposed Rules at 20249.

provider have had a chance to remedy the issue or deploy a fix. This is especially likely given that methods for hacking or cyber-breaches are constantly changing while the tools necessary to protect against such attacks may still need to be developed, or at a minimum, may require additional time to implement.

Further, the level of detail required in the disclosure would result in any ongoing or future vulnerabilities being disclosed to the public before it may be appropriate to do so. For example, the firm may not have yet had a chance to fully investigate or remediate the incident, potentially providing a "roadmap" for future hackers.

The likelihood that public disclosure could lead to more attacks is amplified by the fact that the firms subject to the Proposed Rules are all financial market players that run similar businesses and have similar operational structures. As the Proposal acknowledges, firms "have linkages with each other as a result of the business they conduct together. A breach at one [firm] may be exploited and serve as a means of compromising other [firms]."[12]

For these reasons, the Commission should not adopt the public disclosure requirements as proposed. We believe the Commission should an approach to the public disclosure of cyber incidents that prioritizes the protection of firms from future attacks. Specifically, we ask that, under the final rules, firms are required to publicly disclose information related to a significant cybersecurity incident *only after* the relevant firm has (1) fully investigated the incident and determined its "significance," (2) fully remediated the operational impacts caused by the incident, and (3) adopted tools or mechanisms to enhance the firm's resiliency towards a similar, future attack.

Finally, as suggested in the SIFMA comment letter responding to the Proposal, we ask the Commission to include a law enforcement exemption into the reporting framework for cyber incidents, in recognition of the vitality of cooperation with law enforcement agencies during any potential investigations that arise out of a significant cybersecurity incident.

3. The Commission Should Take a Practical, Outcomes-Based Approach to Substituted Compliance.

ISDA appreciates that the Commission provides an avenue for non-U.S. firms to comply with the requirements of their home country jurisdiction in lieu of the Proposed Rules, where such requirements are comparable to the Proposed Rules. As we have stated in the past in the context of other rulemakings, we encourage the Commission to conduct substituted compliance determinations using an outcomes-based approach that does not require rules to be identical, but rather ensures that similar (but not identical rules) can be deemed comparable as long as they promote the same policy objectives. The comparability review should not look for disparities or variations in the minutiae of foreign regulatory requirements, but rather focus on the manner in

[12] Proposed Rules at 20284-85.

which foreign regulators achieve the objectives of the Proposed Rules, such as establishing a comprehensive cybersecurity risk management framework.

For instance, we do not think it is necessary for non-US SBSDs to submit Form SCIR to the SEC if their home country regulator requires a similar regulatory disclosure. Instead, the firm should be permitted to submit disclosure or reports to the SEC in the same form and manner required by their home country regulator.[13] At a minimum, the Commission should only require non-US SBSDs to submit incident reports to the extent that they affect US operations or US transactions.

In addition, some non-US jurisdictions are still in the process of implementing, their own cyber risk and incident reporting requirements. For example, in the EU, the regulatory directive for the Digital Operational Resilience Act is still in the process of being implemented, along with other discrete non-financial sector specific rules. Thus, we ask the Commission to also take into consideration those rules that are forthcoming, but not fully in effect, when making substituted compliance determinations, or at a minimum, provide interim relief to non-US SBSDs until such rules come into effect and the Commission is equipped to make a substituted compliance determination. [14]

Moreover, substituted compliance determinations are a key planning component for non-US market participants. In order to be meaningful, substituted compliance determinations need to be made well-ahead of the compliance date so that non-US firms can make adjustments to their implementation plans and compliance processes based on such a determination. Issuing substituted compliance determinations after, or close to, the compliance date would not be useful as non-US firms would have likely already implemented the necessary infrastructure, adjusted their policies and procedures, and expended costs to ensure their compliance with the final rules.

Ensuring that substituted compliance is granted via an outcomes-based review and well-ahead of the compliance date for the Proposed Rules will achieve the Commission's objective of ensuring that the Proposed Rules takes into consideration the global nature of the financial market and the prevalence of cross-border transactions.[15]

4. There Should be a Safe Harbor for Firms Subject to Similar Regulations Imposed by Other U.S. Regulators.

As the Commission has proposed to defer to its foreign regulatory counterparts by offering to conduct substituted compliance determinations where appropriate, we believe that the Commission should impose a safe harbor that would allow firms to comply with the cybersecurity requirements of another US regulatory authority in lieu of the SEC's requirements,

[13] In this regard, we also ask that the SEC confirm that the required scope of reporting be limited to significant cybersecurity incidents related to the registered SBSD's activities only.
[14] In line with this flexibility, we do not think that it would be necessary for the SEC to obtain separate memorandums of understanding (MOUs) in order to grant substituted compliance. Instead, the Commission should be able to rely on existing MOUs that are in place for other rules that apply to non-US SBSDs.
[15] Proposed Rules at 20266.

where the firm is subject to both the SEC and the other regulator's cybersecurity rules. This is particularly necessary given that many entities subject to the Proposed Rules are also regulated by the Commodity Futures Trading Commission ("**CFTC**") or form part of larger financial institutions that are subject to the regulations of the federal banking agencies. Additionally, some firms may also be considered critical infrastructure sector entities subject to CIRCIA's requirements.[16]

Creating a safe harbor for firms that are subject to cybersecurity regulatory frameworks imposed by other U.S. regulators will reduce the complexity and cost of complying with similar but not identical regulatory regimes, without compromising the objective to ensure that financial institutions have appropriate policies, procedures and mechanisms in place to avoid and promptly respond to cybersecurity incidents.

Requiring the same firms to comply with two sets of rules that are intended to achieve the same outcomes only introduces regulatory complexity, costs, and compliance challenges without commensurate benefit to regulatory oversight. Thus, ISDA recommends that the Commission provide deference to its fellow US financial regulators and create a safe harbor for firms that are subject to multiple cybersecurity regulatory regimes.[17]

5. Creating Cyber Policies and Procedures Based on the Actions of Third-Party Service Providers Poses Compliance Challenges.

Under the Proposed Rules, a firm is required to evaluate its service providers' practices as part of the firm's cyber risk assessment, including how the service provider protects itself against risks and the service provider's ability to respond to and recover from cybersecurity incidents.[18] While we understand that a firm's engagement with third party service providers has the potential to interject cyber risks to the firm's business, in practice, firms have limited access to their third-party service providers' systems and cybersecurity policies and procedures, making it extremely difficult for firms to conduct a thorough assessment. In some instances, firms may be unable to conduct such an assessment altogether because the service provider is not legally obligated to provide information—let alone detailed information—regarding the service provider's internal policies and procedures. Additionally, firms may not have the expertise to assess the effectiveness of a service provider's cyber security program as such providers offer services to

[16] *See* 6 U.S.C § 681(5), § 681b(c)(1).
[17] Separately, in the context of the rule's application to SBSDs, we ask the SEC to confirm that reporting requirements would only apply to the particular operations and systems of the SBSD (and not other banking systems that are not related to the SBS business). There are portions in the preamble to the Proposed Rules where this is not entirely clear. *Compare* Proposed Rules at 20265 ("Consistent with its approach to the obligations described in Section 15F(j) and to capital, margin, risk mitigation, and recordkeeping, the Commission is proposing to apply the requirements of proposed Rule 10 to an SBS Entity's entire security-based swap business without exception, including in connection with any security-based swap business it conducts with foreign counterparties.") *with* Proposed Rules at 20265 ("Accordingly, the Commission proposes to apply the requirements to the entirety of an SBS Entity's business.").
[18] Proposed Rules at 20240.

various types of market participants and thus have to adjust their risk management practices accordingly.

To make things worse, the Proposed Rules require firms to ensure that service providers adopt similar cybersecurity practices to that of the firm, via a written contract between the service provider and the firm.[19] If finalized, this would have the effect of requiring firms to indirectly regulate their service providers. Needless to say, service providers will be reluctant to provide services under such untenable conditions.[20] Importantly, service providers already have sophisticated cybersecurity programs in place, and firms already conduct effective due diligence.[21] We therefore ask the Commission to reconsider imposing requirements related to the relationship of firms and service providers as it would be impossible for firms to holistically assess their cyber-security programs.

* * * * * * * * * * * * * * *

[19] Proposed Rules at 20242.

[20] Even if a service provider were to agree to amend an existing agreement to comply with the SEC's rules, this will not achieve the Commission's objective to ensure that a service provider has robust cyber-risk management policies as such policies need to be implemented at the enterprise level and not on a contract-by-contract basis.

[21] For example, firms conduct survey across service providers; discuss and review materials provided by service providers; and rely and review service provider certifications, such as the Systems and Organizational Controls certifications issued by American Institute of Certified Public Accountants, which ensures that the entity institutes certain controls with respect to customer data.

ISDA Safe, Efficient Markets

We support the Commission's efforts to establish a cybersecurity risk management framework for the security-based swap markets. We are strongly committed to maintaining the safety and efficiency of financial markets and hope that the Commission will consider our recommendations, as they reflect the extensive knowledge and experience of operational professionals within our membership.

Thank you for your consideration of these concerns. Please do not hesitate to contact me, Nicolette Cone (Associate General Counsel, ncone@isda.org) or Mia Wright (Assistant Director, U.S. Public Policy, mwright@isda.org) should you have any questions.

Bella Rozenberg
Head of Regulatory and Legal Practice Group
ISDA
brozenberg@isda.org