ISDA Safe, Efficient Markets

April 1, 2024 ***Submitted Electronically***

Mr. Christopher Kirkpatrick
Secretary
U.S. Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st St., N.W.
Washington, DC 20581

Re: Operational Resilience Framework for Futures Commission Merchants, Swap Dealers, and Major Swap Participants

Dear Mr. Kirkpatrick:

The International Swaps and Derivatives Association, Inc. (**"ISDA"**)[1] appreciates the opportunity to submit these comments on the Commodity Futures Trading Commission's (**"CFTC or Commission"**) notice of proposed rulemaking (**"Proposal"**) on requirements to establish an Operational Resilience Framework (**"ORF"**) for Futures Commission Merchants, Swap Dealers, and Major Swap Participants, published in the Federal Register on January 24, 2024.[2] As a preliminary matter, we note that our comments relate to the aspects of the Proposal that apply to swap dealers (**"SDs"**), and in this regard, we support the comments put forth by the Securities Industry and Financial Markets Association ("**SIFMA**"), of which we have overlapping membership.

Our members are committed to safe and efficient functioning derivatives markets, and accordingly, currently employ a wide range of safeguards across their respective firms to ensure operational resilience. ISDA commends the Commission for its intent to create a principles-based framework aimed at ensuring firms appropriately identify, monitor, and manage risks relating to information and security technology, third-party relationships, and significant disruptions to business operations. As we have stated in the past,[3] the key to effective risk

[1] Since 1985, ISDA has worked to make the global derivatives markets safer and more efficient. Today, ISDA has over 1,000 member institutions from 76 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 repositories, as well as law firms, accounting firms and other service providers. Information about ISDA and its activities is available on the Association's website: www.isda.org.

[2] Operational Resilience Framework for Futures Commission Merchants, Swap Dealers, and Major Swap Participants, 89 Fed. Reg. 4706-4768 (January 24, 2024) [hereinafter "**Proposal**"].

[3] International Swaps and Derivatives Association and Securities Industry and Financial Markets Association, Letter Re: ANPRM on potential amendments to the Risk Management Program (CFTC Regulations 23.600 and 1.11),

management is understanding the specific vulnerabilities that are particular to a business, and then, creating specific mechanisms to address those risks. A principles-based approach to the regulation of risk is therefore not only welcome, but necessary to enable firms to address operational risks in a manner that is specific to their business. As explained below, we are concerned that certain aspects of the rule run counter to the Commission's intent to ensure operational resilience of its registered entities. Thus, we recommend that the Commission make the following adjustments to its Proposal:

1. **Governance:** provide an alternative to the attestation requirement and revisit the requirement for escalation to the chief compliance officer.
2. **Third-Party Relationships:** the National Futures Association ("**NFA**")'s requirements for third-party service provider programs are already a sufficient safeguard against risk; should the CFTC chose to add an additional layer of regulation, this should be targeted towards high-risk services (rather than all services at the service provider level).
3. **Incident Notification:** revise both the timeline and standard for incident notification.
4. **Implementation Period:** extend the implementation period to allow for more time for compliance and substituted compliance determinations.

We believe that making these adjustments will ensure that the Proposal strikes the right balance between ensuring operational resilience is appropriately accounted for in SDs' risk management programs, while also providing SDs with the necessary flexibility required for effective risk management.

I. Governance

Provide an Alternative to the Attestation Requirement

We appreciate that the Commission recognizes that many SDs function as a division or affiliate of a larger entity or holding company structure,[4] and that, in those cases, many aspects of the Proposal are already managed at the enterprise level. We support that the Proposal allows SDs subject to such a consolidated approach to rely on the programs established at the enterprise level, so long as those programs comply with the Proposal.[5] We disagree, however, that SDs subject to a consolidated approach must always require their senior officer, an oversight body, or senior-level official to attest in writing, on at least an annual basis, that the consolidated program or plan meets the certain requirements of the Proposal.[6] Instead, SDs should have the flexibility to either submit their annual Chief Compliance Officer (**"CCO"**) report in lieu of an attestation or elect to submit an attestation.

(Sept. 18, 2023), available at: https://www.isda.org/2023/09/18/isda-comment-letter-to-cftc-advanced-notice-of-proposed-rulemaking-regarding-risk-management-program-regulations/

[4] Proposal at 4715.

[5] *Id*.

[6] *Id*.

This change would account for the fact that the Commission already has annual audit requirements in place to ensure that all aspects of the Commission's regulations are addressed by the SD.[7] We do not believe that a written attestation is necessary in those instances to achieve the Commission's objectives. Where SDs submit their annual CCO report to the Commission, the Commission should rely on such a report and related requirements to ensure that SDs subscribing to a consolidated plan appropriately account for compliance with the proposed rule.

In addition, non-US SDs should have the flexibility to designate who in their US operations would be responsible for signing an attestation. Such an approach will not only reduce compliance burdens but will also ensure that the individual signing off on compliance has direct knowledge of the program and the SD's US operations.

Furthermore, the Commission should be able to rely on any broad-based program that fully encompasses the SD, regardless of whether this program applies on an "enterprise-wide" or "consolidated" basis. For example, if the program were applicable to the global bank of which the SD is one division but is not also applicable to each of the bank's affiliates (some of which may instead have their own programs), such an approach should not disqualify the relevant program. Similarly, partial reliance on such a broad-based program should be permitted, where a firm demonstrates that some elements of the CFTC rule are addressed at the enterprise-level while others are addressed at the SD-level.

Finally, the Proposal's standard – that the program "meets the requirement of [the rule]" – is overly prescriptive. We believe more flexibility is warranted to allow for the compliance with the consolidated program of other relevant regulatory requirements. We believe the Commission should revise the standard to reflect a principles-based approach; in this regard, a more appropriate standard would be "comparable" or "achieves the same policy outcomes."

For these reasons, we believe the Commission should provide greater flexibility in implementing this requirement by: (1) revising the standard to a more principles-based approach; (2) allowing SDs to either submit their annual CCO report in lieu of an attestation or elect to submit an attestation; and (3) and permitting SDs that are part of a foreign enterprise to have the flexibility to select an appropriate senior management officer of the U.S. operations of the foreign enterprise who is located in the U.S. to provide the attestation.

Revisit the Escalation Requirement to the Chief Compliance Officer

The Proposal requires that SD's incident response plan must include escalation protocols to three roles: (1) either the senior officer, governing board, or the senior level officer responsible for IT; (2) CCO; and (3) any other relevant personnel. We are particularly concerned with the requirement to have incidents escalated to the CCO given the sheer volume of events that could

[7] 17 CFR § 3.3(d)-(e). The CFTC currently requires CCOs to prepare an annual report that includes descriptions of the SD's written policies and procedures required pursuant to the CFTC regulations, the effectiveness of those policies and procedures, areas for improvement, and material noncompliance issues.

qualify as "incidents" under the Proposal[8] and the variety of escalation structures employed by SDs. We believe that escalation to "appropriate senior management" would be more appropriate. Alternatively, we recommend that the CCO receive periodic reporting on incidents to alleviate the potential for unnecessary prescriptiveness in how firms structure their incident response functions. This approach would be more in line with the CCO's function to oversee compliance of all aspects of the SD's operation, as opposed to the Proposal's approach which risks over-involving the CCO in incident response matters that do not rise to the level of a compliance concern and are more appropriately handled by those in the firm with the expertise to swiftly respond to operational issues.

II. Third Party Relationships

The NFA's Requirements are Sufficient to Safeguard Against the Risks Posed by Third-Party Service Providers; Any Additional Requirements should be Appropriately Calibrated to Address Risk

The Proposal contemplates a risk management program for third-party service providers.[9] This program would include requirements related to each step of the third-party relationship lifecycle stages, including risk assessments, due diligence procedures, contractual negotiations, monitoring, and termination; heightened requirements for critical third-party service providers; inventory of third-party service providers; and retention of responsibility by financial institutions.

As the CFTC acknowledges and leverages in the Proposal, the NFA Compliance Rules 2-9(a) and 2-36 and Interpretive Notice 9079 *already* require NFA members to implement a third party service provider program that includes an initial risk assessment, onboarding due diligence, monitoring systems, and recordkeeping.[10] We believe that these requirements are sufficient to address the Commission's concerns regarding the potential risks posed by third-party service providers, and thus, do not see the need for the CFTC to add on an additional layer of regulation.

However, should the CFTC nevertheless impose additional requirements for the oversight of third-party service providers, the proposed rule relating to "heightened requirements" for "critical third-party service providers" should be recalibrated to target risk more appropriately.

While certain services supplied by a third-party service provider may indeed be "critical" to an SD, it is also quite common for that same third-party service provider to supply the SD with a

[8] In this regard, we strongly support the comments of SIFMA, that a number of the Proposal's definitions, including the proposed definition for "incident" are extremely broad and would benefit from re-drafting, especially given the Commission's objectives to develop a principles-based ORF.
[9] *See* Proposal at 4722-4725.
[10] NFA Compliance Rules 2-9, 2-36; Interpretive Notice 9079 (available at https://www.nfa.futures.org/rulebooksql/rules.aspx?Section=9&RuleID=9079).

range of services, many of which carry minimal inherent risk, importance or resilience implications to the SD. To account for this, a more targeted approach is needed to identify third-party *relationships* that require additional due diligence. This approach would avoid unnecessarily scoping-in lower risk services provided by that same third-party service provider.

Thus, the proposed "heightened requirements"[11] rule should be modified by shifting the focus of what is "critical" from the provider-level to the actual service that is being delivered by the third-party service provider. This would result in enhanced due diligence requirements applying only to those services that have the potential to significantly disrupt operations, or significantly impact an SD's customers.

Allow Compliance with the Third-Party Inventory Requirements on an Enterprise Level

Under the Proposal, SDs would be required to create, maintain, and regularly update an inventory of third-party service providers they have engaged to support their activities as a covered entity, identifying whether each third-party service provider in the inventory is a critical third-party service provider.[12] Currently, in most cases, SDs' inventories of third-party service providers are already maintained at the enterprise level, and such an approach is consistent with the recent interagency guidance on third-party service providers promulgated by the federal banking regulators.[13] ISDA similarly believes third-party relationships should be inventoried at the enterprise level, and accordingly, maintaining a copy of the enterprise-level inventory should be sufficient for compliance under the Proposal. Listing all critical third-party service providers at the enterprise-level will provide a clearer picture of all the relationships involved and present less of a compliance challenge to SDs who must comply with the requirement. Additionally, this approach would prevent work from being unnecessarily duplicated within an SD's enterprise.[14]

III. Incident Notification

The Timeframe for Incident Notification Should be 72-Hours

The Proposal's requirement that firms provide written electronic notice of incidents to the CFTC within 24 hours would negatively impact the firms' ability to respond to significant cybersecurity incidents efficiently and effectively.[15] For the reasons articulated below, a 72-hour timeframe, beginning once an SD determines that an incident has adversely impacted the dealer would be more appropriate.

---

[11] Proposal at 4722.
[12] *Id*.
[13] 88 Fed. Reg. 37920-37937 (June 9, 2023).
[14] Notably, the Commission recognized the value of implementing systems at an enterprise level in regards to the consolidated program or plan under Proposed Paragraph (c)(4). (*See* Proposal at 4715).
[15] Proposal at 4731.

At the onset of a significant cybersecurity incident, a firm must have access to all its resources so that it can focus on understanding the extent of the incident and assessing and coordinating the firm's response. Requiring such a quick time period for regulatory notice will divert staff and resources towards fulfilling that obligation, rather than focus on 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 incident.

In addition, cybersecurity incidents are an industry-wide concern. The CFTC should set out reasonable timelines that are in line with other regulators to allow firms to focus on resolving incidents, instead of meeting superficial deadlines that may sidetrack from achieving 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. Reporting the same incident at different times to different regulators is not only burdensome and confusing but may encourage cursory analysis that would prevent the CFTC from getting the most accurate information.

For example, the NFA issued an Interpretive Notice on Information Systems Security Programs which requires reporting of cyber incidents "promptly" (and not "immediately") after their occurrence.[16] The federal banking agencies require notification no later than 36 hours after a firm determines a "notification incident" has occurred and take an 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.[17] Further, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (**"CIRCIA"**) provides for a 72-hour window to report a cybersecurity incident.[18] The CIRCIA requirement 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, inaccurate, and/or incomplete report in order to ensure compliance with the notification requirement.

---

[16] NFA Compliance Rules 2-9, 2-36, and 2-49; Interpretive Notice 9070: Information Security Programs (Aug. 20, 2015), available at: https://www.nfa.futures.org/rulebooksql/rules.aspx?RuleID=9070&Section=9

[17] 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.").

[18] 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.").

For these reasons, ISDA recommends that the CFTC adopt a more flexible approach in calibrating the notification window, like the approaches taken by the NFA, the federal 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, starting from when a firm has determined an incident requires regulatory notification.

The Standard for Incident Notification is Too Broad and Should be Triggered Only by an Actual Adverse Impact

The Proposal requires notification to the Commission of any incident "that adversely impacts, or *is reasonably likely to adversely impact*, (A) information and technology security, (B) the ability of the covered entity to continue its business activities as a covered entity, or (C) the assets or positions of a customer or counterparty."[19]

ISDA believes that the standard should omit the "reasonably likely" language, as its inclusion makes the standard too broad. In an event where a breach or other incident is reasonably likely to have such an impact, firms should be committed to mitigating the risk of that impact without the distraction of complying with the proposed notification requirements. Firms have sophisticated systems in place to respond to such incidents as they happen and can usually address such problems more quickly than it would take to determine the potential, "reasonably likely" impact of an incident. Moreover, such a broad standard may result in firms over-reporting potential incidents, which could pose administrative burdens to the Commission and would run counter to the Commission's objective of exercising its oversight function over those particular incidents that have industry-wide impacts.

To reiterate, SDs should only be required to notify the Commission (within 72-hours) *after* the SD determines an incident has *already* adversely impacted the SD's IT security, ability to continue its business activities, or the assets or positions of a customer. We also agree with other regulatory regimes[20] where notification is only be required for incidents that cause material adverse impact. Either approach would apply a clear, bright line test for notification and is more suitable than a standard where there is room for interpretation on the part of both the Commission and the SD on what may or may not be "reasonably likely" to occur. Moreover, limiting the scope of the notification requirement to incidents with material adverse impact reduces the risk of the Commission's being unnecessarily overwhelmed with notifications of

[19] Proposal at 4731.

[20] *See, e.g.,* 12 C.F.R. §§ 53.2(b)(4), (b)(7), 53.3 (establishing notification requirements for computer security incidents that consider whether an incident has resulted in "actual harm" and whether the incident has "materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade," certain aspects of a banking organization's business).

incidents that do not pose the type of systemic threat that would be of the most interest to the Commission.

The Commission Underestimates the Total Time Required to Report Incidents

The CFTC anticipates that fulfilling the notification requirement for a reportable incident would take approximately 10 hours.[21] We believe the time required is likely much longer, and one reportable incident per year may be an overly optimistic assumption. The Commission should provide a rationale for the estimates included in the Proposal as both the number of incidents and hours required likely underestimate the total compliance burden for SDs.

IV. Implementation Period

The Proposal's Implementation Period Should Be Extended to Allow for More Time for Compliance and Substituted Compliance Determinations.

The Proposal provides for a six-month implementation period.[22] ISDA recommends extending this implementation period for at least one year because the Proposal presents an entirely new framework requiring significant work across various aspects of firms – legal, compliance, operational, and information technology. These efforts would be challenging, and potentially impossible to implement within six months.

The proposed implementation timeline is particularly problematic for non-U.S. swap dealers who would be subject to this rule. While the Commission appropriately designates the Proposal as a "Category A"-level requirement, enabling substituted compliance for non-US SDs,[23] six months will not be enough time for (1) non-US SDs or their regulators to file for substituted compliance; (2) the Commission to review the submissions of multiple jurisdictions; and (3) the Commission to enter into comparability determinations where appropriate. If comparability determinations are not put in place prior to the compliance date, non-U.S. SDs will have to build out interim compliance systems for a rule they would only have to demonstrate exact compliance with for a limited period of time, an expensive and ultimately wasteful exercise.

Separately, but equally important, 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 achieve 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 which foreign

[21] Proposal at 4737.
[22] Proposal at 4735.
[23] Proposal at 4734.

regulators achieve the objectives of the Proposal, such as establishing a comprehensive cybersecurity risk management framework.

* * * * *

We appreciate the opportunity to submit our comments in response to the Proposal. ISDA is strongly committed to maintaining the safety and efficiency of the U.S. swaps markets. We hope that the Commission will consider our suggestions, as they reflect the extensive knowledge and experience of risk management professionals within our membership.

Sincerely,

Bella Rozenberg
Senior Counsel and Head of Legal and Regulatory Practice Group
ISDA