BANK POLICY INSTITUTE

April 1, 2024

Via Electronic Submission

Christopher Kirkpatrick
Secretary
Commodity Futures Trading Commission
Three Lafayette Center
1155 21st Street, NW
Washington, DC 20581

Re: Operational Resilience Framework for Futures Commission Merchants, Swap Dealers, and Major Swap Participants, RIN 3038-AF23

Dear Mr. Kirkpatrick:

The Bank Policy Institute[1] welcomes the opportunity to respond to the notice of proposed rulemaking by the Commodity Futures Trading Commission to require futures commission merchants ("FCMs"), swap dealers ("SDs") and major swap participants (collectively with FCMs and SDs, "covered entities") to establish, document, implement, and maintain an operational resilience framework.[2] We appreciate the Commission's focus on this area. Appropriate management of risks relating to information and technology security, third-party relationships, and emergencies or other significant disruptions to normal business operations has likewise been a significant focus for banking organizations and their prudential regulators for many years.

---

[1] The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost two million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

[2] Operational Resilience Framework for Futures Commission Merchants, Swap Dealers, and Major Swap Participants, 89 Fed. Reg. 4,706 (Jan. 24, 2024) (the "Proposing Release").

We further support the Commission's efforts to draw on the approaches adopted by the prudential regulators in this area when formulating its proposed rules[3] and its proposal that substituted compliance with comparable home country rules should broadly be available for non-U.S. SDs and major swap participants.[4] We also note the Commission's proposal to permit covered entities, under certain conditions, to satisfy certain aspects of the proposed rules through participation in a consolidated program or plan managed and approved at the enterprise level.[5]

These measures will not be sufficient, however, to avoid regulatory conflicts and inefficiencies. Several inconsistencies remain between the proposed rules and relevant prudential regulator rules and guidance. These inconsistencies are likely to expand in practice through divergent examination and supervision processes. We believe that substituted compliance is an effective way to address these issues, and we urge the Commission to adopt a principles-based approach towards substituted compliance that focuses on holistic outcomes. But substituted compliance standing alone will not fully address these issues because it would not be available to U.S. covered entities. The proposed treatment of consolidated programs and plans also would not address these issues for U.S. covered entities because it has multiple significant flaws, which could actually increase the extent of regulatory conflicts and inefficiencies.

Below we provide additional details concerning these issues. We also make recommendations for how the Commission could tailor the proposed rules' provisions concerning participation in consolidated programs and plans to account better for circumstances where covered entities are already subject to comprehensive regulation and supervision of their operational resilience by U.S. prudential regulators.

I. The Proposed Rules Would Overlap with Existing U.S. Prudential Regulation

The proposed rules would require a covered entity to establish, document, implement, and maintain an operational resilience framework with three components: an information and technology security program, a third-party relationship program, and a business continuity and disaster recovery plan. These components would be supported by broad requirements relating to governance (including senior-level approval of each component along with risk appetite and risk tolerance limits), training, testing, and recordkeeping. Covered entities would also be required to notify the Commission, customers, and counterparties regarding certain events.

Most of the U.S. entities subject to these requirements are already subject to supervision by a U.S. prudential regulator directly or at a consolidated holding company level.

---

3 *See id.* at 4,710.

4 *Id.* at 4,734.

5 *Id.* at 4,715-16.

Of the roughly 43 U.S. registered SDs (out of a total of 107 registered SDs), 30 are either banks with a U.S. prudential regulator or nonbank subsidiaries of a bank holding company regulated by the Federal Reserve Board. Roughly 20 of the 62 registered FCMs are also subsidiaries of a bank holding company regulated by the Federal Reserve Board.

As the Commission itself observes,[6] the U.S. prudential regulators have adopted extensive rules and guidance concerning operational resilience. These rules and guidance cover the same areas as the proposed rules.[7] In addition, because they apply at an enterprise-wide level, they cover not only firms' core banking businesses but also the SD and FCM businesses that the proposed rules would cover. So, for these prudentially regulated covered entities, existing prudential regulator rules and guidance would overlap with the proposed rules' coverage.

II. The Proposed Rules Would Result in Undesirable Regulatory Conflicts and Inefficiencies

Although the Commission took into account the prudential regulators' rules and guidance when developing the proposed rules, several inconsistencies remain. For example, the proposed rules contain several prescriptive requirements around risk assessments, including that they be conducted by independent personnel, which prudential regulators do not require[8] and could inhibit appropriate engagement by qualified first-line of defense personnel.

The Commission's proposal also conflicts with the prudential regulators' Computer-Security Incident Notification Rule in several meaningful respects. That rule was the product of extensive industry engagement with the banking regulators to align on workable timeframes and scope for confidentially reporting cyber incidents. To limit over-reporting of insignificant or easily remediated incidents, the prudential regulators' rule contains a materiality qualifier and an actual harm standard[9] absent from the notification trigger provisions in the proposed rules.[10] Moreover, when the Computer-Security Incident Notification Rule was first proposed,

---

6 *See id.* at 4,710, n. 11.

7 *See, e.g.*, FRB, OCC, FDIC, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*, 86 Fed. Reg. 66,424 ("Computer-Security Incident Notification Requirements"); FRB, OCC, FDIC, *Interagency Guidance on Third-Party Relationships: Risk Management*, 88 Fed. Reg. 37,920 ("Interagency Guidance on Third-Party Relationships"); FRB, OCC, FDIC, *Interagency Guidelines Establishing Standards for Safety and Soundness*, 12 CFR § 208, Appendix D-1; FRB, OCC, FDIC, *Interagency Guidelines Establishing Information Security Standards*, 12 CFR § 30, Appendix B; FRB, OCC, FDIC, *Interagency Paper on Sound Practices to Strengthen Operational Resilience* (November 2, 2020); FFIEC, *Business Continuity Management*, FFIEC IT Examination Handbook (November 14, 2019).

8 *See* FFIEC Examination Handbook Infobase, *Information Security – Risk Measurement.*

9 *Computer-Security Incident Notification* at 66,442-66,444.

10 Proposing Release at 4,753.

industry was clear its 36-hour notification requirement would not be achievable unless the notification did not require an assessment of the incident.[11] The Commission's proposal not only requires covered entities to provide incident assessments, but to do so no later than 24 hours after detection.[12] Such a requirement is at odds with the realities of early-stage incident response efforts and would unnecessarily divert critical security resources to compliance activities rather than remediation and protecting against further harm.

Even if the Commission eliminated those inconsistencies before finalizing the rules, prudentially regulated covered entities would remain subject to overlapping examination and supervision. At a minimum this overlap would lead to inefficient use of limited agency resources, as examiners from multiple agencies review the same policies and processes. More troubling is the prospect of inconsistent findings and supervisory directions arising from differing views about such topics as which system safeguards to employ, what provisions to include in contracts with third parties, whether or when to terminate third-party relationships, or other measures to remediate open issues.

Also, it should be expected that the Commission and the U.S. prudential regulators will publish additional guidance over time as relevant technologies and industry standards evolve. As a consequence, harmonization at a single point in time will not be a sufficient step to prevent the emergence of conflicts or other inconsistencies in the future.

III. We Support Substituted Compliance, But It Would Not Adequately Address These Issues

The proposed rules envision that a non-U.S. SD or major swap participant could satisfy the rules through substituted compliance with comparable home country rules.[13] If such a non-U.S. entity qualifies for substituted compliance, then it will not bear the burden of regulatory inconsistencies described above. In addition, under the current approach to examinations followed by the Commission and National Futures Association, pursuant to which they generally focus on requirements for which substituted compliance is <u>not</u> found,[14] these non-U.S. entities also will not experience conflicting examination feedback like U.S. prudentially regulated entities might experience.

---

[11] Bank Policy Institute et. al, Comment Letter on Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers (Apr. 12, 2021), https://bpi.com/wp-content/uploads/2021/04/Consumer-Security-Incident-Notification-Reqs-for-Banking-Organizations-and-Their-Bank-Service-Providers-2021.04.12.pdf.

[12] Proposing Release at 4,753.

[13] Proposing Release at 4,734.

[14] *See* 85 Fed. Reg. 59, 624, 59, 679 (Sep. 14, 2020).

For non-U.S. SDs, the ability to rely on substituted compliance is imperative to avoid the regulatory overlaps and inconsistencies described in this letter. We strongly support the Commission's proposal to allow for reliance on home country requirements, and urge the Commission to apply a principles-based approach to substituted compliance that focuses on outcomes rather than exact matches. Substituted compliance determinations also must be made by the Commission in a timely manner, subject to a sufficient implementation window to avoid potential gaps.

However, while we fully support the application of substituted compliance for non-U.S. entities to the proposed rules, we are concerned that no similar relief would be afforded to U.S. prudentially regulated entities, thus causing them to receive less regulatory deference than non-U.S. entities. To avoid this odd and indefensible result, the Commission should exercise the same deference to U.S. prudential regulators as it does to foreign regulators, allowing U.S. prudentially regulated entities to comply instead with applicable operational risk requirements of the prudential regulators, as described in Part V below.

IV. The Proposal to Permit Reliance on Consolidated Programs or Plans Would Not Address These Issues

The Commission acknowledges that many covered entities function as a division or affiliate of a larger entity or holding company structure for which operational risks are monitored and managed at the enterprise level to address the risks holistically and to achieve economies of scale.[15] In recognition of the benefits of such a consolidated approach and to avoid interference with covered entities' operational structures, the proposed rules would permit a covered entity to satisfy certain aspects of the proposed rules through participation in a consolidated program or plan, under specified conditions.[16] Specifically, a covered entity could satisfy requirements for an information and technology security program, a third-party relationship program, or a business continuity and disaster recovery plan through participation in a consolidated program or plan, provided that (i) the consolidated program or plan meets all the requirements of the proposed rules and (ii) the covered entity's senior officer, oversight body, or senior-level official annually attests that the consolidated program or plan meets the requirements of the proposed rules and reflects a risk appetite and risk tolerance limits appropriate for the covered entity.[17]

Although well-intentioned, this aspect of the proposed rules would not achieve its intended objectives. The conditions a covered entity would need to satisfy to rely on a consolidated program or plan would largely undermine the benefits of a consolidated approach and result in substantial interference with covered entities' enterprise-wide programs.

---

15 Proposing Release at 4,715.

16 *See id.*

17 *See id.* at 4,715-16.

First, a covered entity would need to assess, and an officer or body would need to attest annually to, consistency of the consolidated program or plan with the proposed rules. If there was an inconsistency – a possibility that is likely for the reasons set out above – then either the covered entity could not rely on the consolidated program or plan, or it would need to modify that program or plan to follow the Commission's rules. This would result in the sort of interference the Commission is seeking to avoid.

Second, the consolidated level program or plan would need to reflect a risk appetite and risk tolerance limits appropriate to the covered entity. It is not entirely clear what this requirement would entail. If it merely requires that the consolidated program or plan take into account the operational risks associated with the SD or FCM business, then it should not pose a material issue. On the other hand, if it requires a lesser risk appetite and lower risk tolerance limits relative to the overall enterprise merely because the covered entity is but a part of that enterprise, then the requirement would single out those businesses, unique among those conducted by the firm, for special treatment. In effect, this requirement could necessitate a prioritization of resources to mitigate the operational risks of the SD or FCM business relative to the other businesses of the firm, including consumer and commercial lending, deposit-taking, securities brokerage, dealing and investment banking, and so on. We are not aware of any overarching policy or legal justification for such a result, which runs contrary to the benefits of an enterprise-wide program acknowledged by the Commission.

Third, the proposed rules would <u>not</u> permit a covered entity to satisfy the rules' training or testing requirements through participation in a consolidated training or testing program. This limitation seems illogical and possibly unintended. If the entity is otherwise relying on its participation in a consolidated information security or third-party relationship program or business continuity plan, which in turn is the subject of training and testing at an enterprise-level, it is unclear what additional or different training or testing could or should take place at the level of the covered entity. If there are differences due to the proposed rules prescriptively specifying what sorts of training or testing must take place, then this limitation would present the same risks of duplication and interference described above.

V. The Commission Should Enhance the Ability for Prudentially Regulated Firms to Rely on Enterprise-Wide Operational Resilience Frameworks

In order to address the issues discussed by this letter, the Commission should enhance the ability for prudentially regulated covered entities to rely on their enterprise-wide operational resilience frameworks. For this purpose, a covered entity should be considered "prudentially regulated" if it either has a U.S. prudential regulator at the level of the covered entity itself (*e.g.*, in the case of an SD that is a national bank or state member bank) or is subject to consolidated supervision and regulation by the Federal Reserve Board as a subsidiary of a bank holding company. Such a prudentially regulated covered entity should be permitted to satisfy <u>all</u> aspects of the Commission's operational resilience framework rules (<u>except</u> requirements to notify the Commission, customers, or counterparties of specified incidents and

other events) through participation in its consolidated operational resilience framework programs or plans, provided that covered entity satisfies three conditions:

- the covered entity's senior officer, oversight body, or senior-level officer annually attests that the consolidated program or plan is reasonably designed to meet applicable prudential regulator rules and guidance;
- the covered entity annually submits to the Commission a report summarizing the consolidated program or plan and any material changes or areas for improvement; and
- the covered entity makes available to the Commission the written policies and procedures comprising the consolidated program or plan and the results of any internal operational risk assessments or testing.[18]

Such a prudentially regulated covered entity would remain subject to the Commission's proposed notification requirements, but the Commission should harmonize those requirements with other regulators to the greatest extent possible by harmonizing the scope of reportable incidents (*e.g.*, by including a materiality qualifier) and the deadlines for making notifications. Further, for non-U.S. SDs, substituted compliance should allow for adherence to home country notification protocols.

Notably, a prudentially regulated covered entity would not, under this recommendation, need to assess consistency of its consolidated program or plan with the Commission's specific operational resilience framework requirements. Instead, given that the Commission has sought to base its requirements on prudential regulators' rules and guidance, this recommendation would in practice codify a substituted compliance approach for U.S. prudentially regulated covered entities. Such an approach would avoid the regulatory conflicts and inefficiencies described above. However, to ensure that the Commission has adequate transparency into covered entities' operational risks and resilience, prudentially regulated covered entities would remain subject to Commission incident and other notification requirements, and they would be subject to reporting and information availability requirements around the content and implementation of their consolidated programs or plans. If, as a result, the Commission became aware of an operational risk issue, we would envision it could consult and coordinate with the relevant prudential regulator(s) for the entity in question.

*****

[18] In order to comply with applicable law, any such results provided to the Commission would need to redact for confidential supervisory information.

BPI appreciates the opportunity to comment on the proposed rules. If you have any questions, please contact the undersigned by email at tabitha.edgens@bpi.com.

Respectfully submitted,

/s/

Tabitha Edgens
Senior Vice President and
Senior Associate General Counsel
Bank Policy Institute