Commodity Futures Trading Commission
Office of Public Affairs
Three Lafayette Centre
1155 21st Street, NW
Washington, DC 20581
cftc.gov

December 13, 2023

Fact Sheet and Q&A – Notice of Proposed Rulemaking to Require Futures Commission Merchants, Swap Dealers, and Major Swap Participants to Establish an Operational Resilience Framework

The Commodity Futures Trading Commission ("Commission" or "CFTC") is proposing to require that futures commission merchants ("FCMs"), swap dealers ("SDs"), and major swap participants ("MSPs") establish, document, implement, and maintain an Operational Resilience Framework reasonably designed to identify, monitor, manage, and assess risks relating to information and technology security, third-party relationships, and emergencies or other significant disruptions to normal business operations. The Commission is further proposing guidance relating to the management of risks stemming from third-party relationships. The proposed rule would be codified in new Regulation 1.13 for FCMs and existing Regulation 23.603 for SDs and MSPs (collectively, "swap entities"). The proposed guidance relating to third-party relationships would be included as appendices to parts 1 and 23 of the Commission's regulations.

Background

In 2012 and 2013, the Commission adopted rules requiring that FCMs, SDs, and MSPs (collectively, "covered entities") establish a risk management program ("RMP") designed to monitor and manage the risks associated with their activities as covered entities. Recognizing that covered entities vary in size and complexity, the RMP rules identify certain elements that must, at a minimum, be included as part of the RMP, and require that certain enumerated risks be taken into account, but the rules otherwise allow covered entities flexibility to design RMPs tailored to their circumstances and organizational structures.

Based on its decade of experience with the RMP rules, the Commission believes it has identified opportunities to adapt its regulations to further promote sound risk management practices, reduce risk to the U.S. financial system, and protect commodity interest customers and counterparties. Specifically, as it relates to the proposed rule, the Commission has identified a need for more particularized risk management requirements for covered entities designed to promote operational resilience.

An outcome of the effective management of operational risk, "operational resilience" can be broadly defined as the ability of a firm to detect, resist, adapt to, respond to, and recover from operational disruptions. As the use of technology and associated third-party service providers has expanded within the financial sector, so too have the sources of operational risk facing covered entities, notably the potential for technological failures and cyberattacks. The Commission preliminarily believes that requirements for covered entities directed at promoting sound practices for managing these risks, as well as the risk of other potential physical disruptions to operations (*e.g.*, power outages, natural disasters, pandemics), and for mitigating their potential impact would not only strengthen individual covered entity operational resilience, but reduce risk to the U.S. financial system as a whole and help protect derivatives customers and counterparties.

Summary of Proposal

The Commission is proposing to require that covered entities establish, document, implement, and maintain an Operational Resilience Framework ("ORF") reasonably designed to identify, monitor, manage, and assess risks relating to information and technology security, third-party relationships, and emergencies or other significant disruptions to normal business operations. Following the principles-based approach of the RMP rules, the Commission would require that the ORF be appropriate and

proportionate to the nature, size, scope, complexity, and risk profile of its business activities as an FCM, SD, or MSP, following generally accepted standards and best practices.

The ORF would include three key components: an information and technology security program, a third-party relationship program, and a business continuity and disaster recovery ("BCDR") plan. Each of these three components would need to be supported by written policies and procedures and include certain minimum elements, as described in the rule. The ORF would further be supported by broad requirements relating to governance, training, testing, and recordkeeping. Notably, as part of the governance requirement, the proposed rule would require covered entities to establish risk appetite and risk tolerance limits and would allow covered entities to rely on an information and technology security program, third-party relationship program, or BCDR plan in which the covered entity participates with one or more affiliates and that is managed and approved at the enterprise level. Testing would need to be risk-based and include, at a minimum, daily or continuous vulnerability assessment and annual penetration testing, among other testing. The proposed rule would also require certain notifications to the Commission and customers or counterparties.

The Commission is further proposing guidance identifying factors, actions, and strategies for covered entities to consider in preparing and implementing their third-party relationship programs. The guidance is intended to be broadly relevant to all covered entities and would not necessarily be universally applicable. The guidance would be nonbinding.

Proposed Rulemaking Q & A

1. Who would be affected by the proposed rule?

The proposed rule would apply to all FCMs, SDs, and MSPs.

2. What would the proposed rule require?

The proposed rule would require covered entities to establish, document, implement, and maintain an Operational Resilience Framework reasonably designed to identify, monitor, manage, and assess risks relating to information and technology security, third-party relationships, and emergencies or other significant disruptions to the continuity of normal business operations as a CFTC registrant. The Operational Resilience Framework would need to include an information and technology security program, a third-party relationship program, and a BCDR plan.

3. What would be the requirements of the proposed information and technology security program?

The proposed information and technology security plan would need to include: a risk assessment, conducted at least annually; controls reasonably designed to prevent, detect, and mitigate identified risks to information and technology security; and an incident response plan.

4. What would be the requirements of the proposed third-party relationship program?

The proposed third-party relationship program would need to describe how the covered entity would address the risks attendant to each stage of the third-party relationship lifecycle: pre-selection risk assessment; due diligence of prospective third-party service providers; contractual negotiations; ongoing monitoring; and termination, including preparations for planned and unplanned terminations. The plan would also need to establish heightened due diligence practices and ongoing monitoring for critical third-party service providers, and include an inventory of third-party service providers engaged to support its activities as a covered entity, identifying whether each third-party service provider in the inventory is a critical-third-party service provider. With respect to third-party relationships, should this proposal be adopted as final, covered entities would apply their third-party relationship programs across all stages of the relationship lifecycle on a going-forward basis. Although covered entities would not be required to renegotiate or terminate existing agreements, it would expect covered entities to conduct ongoing monitoring of existing third-party service providers consistent with the program and this regulation and, to the extent possible, to rely on its program with respect to termination.

5. What would be the requirements of the proposed BCDR plan?

The proposed BCDR plan requirement is based on the BCDR plan requirement for swap entities in existing Regulation 23.603 with certain proposed amendments. The BCDR plan would need to be reasonably designed to enable the covered entity to

continue or resume normal business operations with minimal disruption to customers and the markets and to recover and make use of covered information, as well as other data, information, or documentation required to be maintained by law and regulation. Unlike current Regulation 23.603, the proposed BCDR plan requirement would not require the BCDR plan to be audited at least once every three years by a qualified third-party service.

6. What testing would the proposed ORF rule require?

The proposed rule would require risk-based testing of the ORF. The frequency, nature, and scope of that testing would generally need to be appropriate and proportionate to the nature, size, scope, complexity, and risk profile of its business activities as a covered entity, following generally accepted standards and best practices. The proposed rule would also specifically require that testing of the information and technology security program include testing of key controls and the incident response plan at least annually; vulnerability assessments, including daily or continuous automated vulnerability scans; and penetration testing at least annually. Testing of the BCDR plan would need to include a walk-through or tabletop exercise designed to test the effectiveness of backup facilities and capabilities at least annually. The testing would need to be conducted by qualified personnel who are independent of the component of the ORF being reviewed or tested.

7. What notifications would the proposed ORF rule require?

The proposed rule would require covered entities to notify the Commission of any incident that adversely impacts, or is reasonably likely to adversely impact: information and technology security; the ability of the covered entity to continue its business activities as a covered entity; or the assets or positions of a customer or counterparty. Covered entities would also need to notify the Commission of any determination to activate their BCDR plan. Notifications to the Commission would function as an early warning and would need to include information available to the covered entity at the time of the notification that may assist the Commission in assessing and responding to the incident. Notifications to the Commission would need to be provided as soon as possible, but in any event, no later than 24 hours after the incident has been detected or the BCDR plan has been activated, as appropriate.

Customers or counterparties would need to be notified as soon as possible of any incident that is reasonably likely to have adversely affected the confidentiality or integrity of their covered information, assets, or positions. The notification would need to include information necessary for the affected customer or counterparty to understand and assess the potential impact of the incident on its information, assets, or positions and to take any necessary action, including, at a minimum, a description of the incident; the particular way in which the customer or counterparty, or its covered information, may have been adversely impacted; measures being taken by the covered entity to protect against further harm; and contact information for the covered entity where the counterparty may learn more about the incident or ask questions.

8. If a covered entity is a division or affiliate of a larger entity or holding company structure that monitors and manages operational risks through a consolidated program or plan, can that covered entity satisfy the component program or plan requirement by participating in the consolidated program or plan?

Yes. A covered entity that functions as a division or affiliate of a larger entity or holding company structure that monitors and manages operational risks through a consolidated program or plan may satisfy the component program or plan requirement through its participation in a consolidated program or plan, provided the consolidated program or plan meets the requirements of the proposed rule. The senior officer, an oversight body, or a senior-level official of the covered entity would be required to attest in writing, on at least an annual basis, that the consolidated program or plan meets the requirements of this section and reflects the risk appetite and risk tolerance limits the covered entity has established under the rule. This is intended to ensure that such enterprise-level ORF appropriately addresses the risks specific to the covered entity, and that such covered entities are on equal footing with those not part of a larger entity or holding company structure.