RIN Number 3038-AF23

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

I am writing to provide comments on the proposed rule on operational resilience framework for futures commission merchants, swap dealers, and major swap participants (covered entities) issued by the Commodity Futures Trading Commission (CFTC).

I suggest including examples of operational disruptions that may affect the operational resilience of covered entities or the financial system. In my opinion, providing such examples in the proposed rule would be helpful and informative for covered entities and other stakeholders, as they would illustrate the types, causes, and impacts of operational disruptions, and how covered entities can apply the operational resilience framework to prevent, mitigate, or recover from them. This would also support a flexible approach well-suited to an evolving threat landscape.

However, the CFTC should clearly state that the examples are not intended to be a comprehensive or exhaustive list of all possible operational disruptions, and that covered entities should identify and assess their own operational risks and resilience based on their specific circumstances and environment. The CFTC should also emphasize that the examples are not binding or prescriptive, and that covered entities should use their own judgment and discretion in designing and implementing their operational resilience framework in accordance with generally accepted standards and best practices.

Some examples of operational disruptions that the CFTC could mention in the proposed rule are:

- A power outage causing widespread system failures and rendering a covered entity's critical IT systems unavailable.
- A data breach that results in the unauthorized release of sensitive customer information and damage to the covered entity's reputation.
- A natural disaster, such as a hurricane, a flood, or a wildfire, that damages or destroys the covered entity's facilities, equipment, or infrastructure, or disrupts its supply chain or transportation network.
- A cyberattack, such as a ransomware, a denial-of-service, or a phishing attack, that compromises or disables the covered entity's information and technology systems, or those of its third-party service providers.

- A market disruption, such as a financial crisis, a trade war, or a pandemic, that affects the demand, supply, or price of the covered entity's products or services, or creates volatility or uncertainty in the financial system.

- A "flash crash", i.e., a sudden and sharp drop in the value of a market or a security, triggered by a large volume of algorithmic-driven automated orders or a glitch in the trading system, followed by a quick recovery within minutes or hours.

- A labor strike or a civil unrest that prevents or delays the delivery or receipt of goods or services, or disrupts the normal operations or communications of the covered entity or its third-party service providers.

- A hardware or software malfunction or failure that causes data loss, corruption, or inaccuracy, or impairs the functionality or performance of the covered entity's information and technology systems, or those of its third-party service providers.

- A legal or regulatory change or action that significantly affects the compliance obligations, contractual rights, or operational requirements of the covered entity or its third-party service providers, or creates uncertainty or inconsistency in the legal and regulatory environment.

Such examples would help the affected markets participants to assess their information and technology security program, third-party relationship program, and business continuity and disaster recovery plan against potential disruption scenarios, but would not be prescriptive or restrictive.

Michael Ravnitzky
Silver Spring, Maryland