



BETTER MARKETS

By Electronic Submission

April 1, 2024

Christopher Kirkpatrick
Secretary of the Commission
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, N.W.
Washington, DC 20581

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

Dear Mr. Kirkpatrick:

Better Markets¹ appreciates the opportunity to comment on the Commodity Futures Trading Commission’s (“CFTC” or “Commission”) proposed rulemaking² (“Proposed Rule”) proposing to require that futures commission merchants (FCMs), swap dealers (SDs), and major swap participants 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.

Operational resilience extends beyond traditional disaster recovery and business continuity planning. It encompasses a holistic approach to managing a range of risks, including cybersecurity threats, technology failures, and supply chain vulnerabilities. For FCMs and SDs, this means not only having robust systems in place but also ensuring that they can quickly adapt and respond to rapidly evolving threats and challenges. The implementation of an ORF would require these firms to regularly test their systems and processes, ensuring they can withstand a variety of stress scenarios.

¹ Better Markets is a non-profit, non-partisan, and independent organization founded in the wake of the 2008 financial crisis to promote the public interest in the financial markets, support the financial reform of Wall Street, and make our financial system work for all Americans again. Better Markets works with allies—including many in finance—to promote pro-market, pro-business, and pro-growth policies that help build a stronger, safer financial system that protects and promotes Americans’ jobs, savings, retirements, and more.

² Operational Resilience Framework for Futures Commission Merchants, Swap Dealers, and Major Swap Participants; 89 Fed. Reg. 4706 (January 24, 2024).

The Proposed Rule outlines a detailed ORF, emphasizing the need for an information and technology security program, a third-party relationship program, and a business continuity and disaster recovery plan.³ These key components, reinforced by governance, training, testing, and recordkeeping protocols, highlight the comprehensive and proactive approach required for effective operational resilience. Additionally, the rule mandates timely notifications to the Commission and stakeholders, reinforcing the need for transparency and accountability in operational risk management.⁴

In fulfilling its Dodd-Frank mandate, the Commission adopted rules requiring FCMs and SDs to implement Risk Management Programs that reflect the evolving nature of risk management in the financial sector. These entities were required to design RMPs that adequately monitored and managed risks pertinent to their operations, with allowances for flexibility based on their size and complexity. This flexibility proved essential as the financial sector navigated various global and economic challenges, including Brexit, the LIBOR transition, and the COVID-19 pandemic.

The experience gained by the Commission over the past decade confirms the effectiveness of the RMP rules in building resilience, enabling entities to manage and recover from market disturbances. This experience underscores the foundation that RMP rules provide in enhancing risk management practices, which in turn reduce systemic risk. The ORF proposed by the CFTC aims to leverage this established foundation, enhancing the operational resilience of FCMs and SDs against an ever-changing financial backdrop. The Proposed Rule is thus an essential step towards enhancing the overall resilience of the financial system, ensuring that FCMs and SDs are better equipped to manage and mitigate operational disruptions.

Nevertheless, Better Markets strongly opposes the CFTC's substituted compliance approach, particularly concerning the extension of regulation 23.603, which encompasses the proposed operational resilience framework. Allowing foreign firms to adhere to U.S. regulatory standards through substituted compliance, especially for crucial aspects like operational resilience, is a significant flaw, potentially compromising the U.S. financial market's integrity. Given the financial system's interconnected nature, individual firms' operational resilience is paramount, highlighting the ORF's role in bolstering financial stability. Therefore, the expansion of regulation 23.603 should mandate direct and stringent regulatory compliance to safeguard against systemic risks effectively. Better Markets urges the CFTC not to allow substituted compliance for these expanded regulations. In fact, the CFTC should re-evaluate its substituted compliance approach in order to fortify the regulatory mechanisms protecting the financial system. This is essential not only for the entities directly involved but also for safeguarding the broader public.

BACKGROUND

Testifying before the U.S. Senate Committee on Homeland Security and Governmental Affairs, the Director of the agency charged with managing and mitigating cybersecurity risks to critical infrastructure, the Cybersecurity and Infrastructure Security Agency (“CISA”), stated that

³ See The Proposed Rule, 89 Fed. Reg. 4706

⁴ *Id.*

the U.S. is facing “unprecedented risk from cyberattacks undertaken by both nation-state adversaries and criminals.”⁵ The financial industry and its participants are prime targets of cyberattacks and data breaches, and those risks are increasing. In fact, the average cost to a financial company of a cyberattack is 40% higher than the average cost to companies in other sectors.⁶ As the financial industry is a natural target for cyberattacks, the Financial Stability Oversight Council (“FSOC”) has increasingly discussed cyberattacks as a threat to the stability of the U.S. financial system in their annual reports to Congress, stating “incidents have the potential to impact tens or even hundreds of millions of Americans and result in financial losses of billions of dollars due to disruptions in operations, theft, and recovery costs.”⁷

Just as we have seen the economic damage a global pandemic can have on companies of all sizes, we have also seen the crippling effects a major cyberattack or data breach can have on a company. For example, we saw the largest gas pipeline operator and the largest meat processing plant in the U.S. each forced to halt operations due to a pair of cyberattacks in 2021. These cyberattacks cut off 45% of the oil to the East Coast and halted production at a company that provides one-fifth of the U.S.’s meat supply.⁸ In addition, malware and ransomware attacks increased in 2020 by 358% and 435%, respectively, from the previous year.⁹ When you combine the debilitating consequences of a successful cyberattack, combined with the relentless threat of attack, it is no wonder cybersecurity is the top threat to U.S. companies cited by CEOs. Unfortunately, this trend can be expected to increase as businesses become more dependent on digitizing their operations and storing more and more valuable data within their networking systems. This increased reliance on digitized data will create increasingly attractive targets for cybercriminals, motivating them to ramp up their cyberattacks.

For each data breach, experts have estimated that the average cost *per record* breached was \$164 in 2022, a 16.3% increase since 2017.¹⁰ While \$164 per record may not seem like a large sum of money in isolation, it actually suggests huge collective costs, as cybercriminals are less likely to target individuals and more likely to target businesses and organizations with vast troves of data representing thousands and millions of records. The average cost of a data breach in the United States in 2022 was \$9.44 million, while the average cost of a ransomware attack in 2022, prior to any ransom being paid, was \$4.54 million.¹¹ This number also does not account for the

⁵ *National Cybersecurity Strategy: Protection of Federal and Critical Infrastructure Systems: Hearing Before the S. Committee on Homeland Security & Governmental Affairs*, 117th Cong. (2021) (statement of Jen Easterly, Director, Cybersecurity and Infrastructure Security Agency).

⁶ ANDREW P. SCOTT AND PAUL TIerno, CONG. RSCH. SERV., IF11717, INTRODUCTION TO FINANCIAL SERVICES: FINANCIAL CYBERSECURITY (Jan. 13, 2022), <https://crsreports.congress.gov/product/pdf/IF/IF11717>.

⁷ FSOC, *supra* note 13 at 168. FSOC goes on to highlight three channels through which financial stability could be threatened: disruption of a key financial service or utility with little or no substitute; compromised integrity of market data; and loss of consumer or investor confidence in markets that affects the safety and liquidity of assets.

⁸ See Financial Stability Oversight Council, Annual Report (2021), available at <https://home.treasury.gov/system/files/261/FSOC2021AnnualReport.pdf>.

⁹ World Economic Forum, *supra* note 5 at 9.

¹⁰ IBM, Cost of a Data Breach Report 9 (2022), <https://www.ibm.com/downloads/cas/3R8N1DZJ>.

¹¹ *Id.* at 6-7.

financial damage wreaked on the individual consumer or investor who has had their sensitive information breached, which can be debilitating and devastating. In the case of large breaches, the financial damage of a cyberattack or data breach can have consequential and systemic consequences not only in the markets but also on society as a whole.

The COVID-19 pandemic and the changes in the modern workplace that have come as a result of the pandemic have only elevated the risk of cyberattacks. The increase in remote work has made companies and organizations more vulnerable to cyberattacks through the increased use of teleworking strategies, including virtual meeting applications and virtual private networks. Research has found that data breaches where remote work was a factor in the breach increased the total cost of a breach by nearly \$ 1 million on average.¹² This raises the level of vigilance that all market participants must maintain in connection with cybersecurity vulnerabilities and further demonstrates the growing risk cybersecurity poses to society.

For example, In 2023, the cybersecurity landscape saw significant breaches, including an attack on AT&T that exposed the personal details of approximately 9 million customers and a vulnerability in a TmaxSoft Kibana dashboard that exposed over 56 million sensitive records.¹³ These incidents contributed to a staggering total of over 5 billion records breached throughout the year, with October alone accounting for 867,072,315 compromised records across 114 publicly disclosed security incidents.¹⁴

The financial repercussions of these breaches have been profound, with the cost of data breaches in the United States reaching new heights. This financial strain is further compounded by a notable 600% increase in cyberattacks targeting cryptocurrency firms and a significant rise in DDoS attacks.¹⁵ The average ransomware payout also saw a dramatic increase, more than doubling from the previous year, illustrating the escalating financial stakes of cyber incidents.

One of the notable cyberattacks of 2023 was on the ION Group, executed by the LockBit ransomware gang.¹⁶ This attack severely disrupted the derivatives trading market, affecting ION Cleared Derivatives and forcing significant customers in the United States and Europe to manually process trades. The incident highlighted the risks associated with third-party service providers in the financial sector, underscoring the critical need for robust cybersecurity measures and protocols.

¹² *Id.* at 6.

¹³ See Rob Sobers, *161 Cybersecurity Statistics and Trends [updated 2023]*, VARONIS (January 4, 2024), available at <https://www.varonis.com/blog/cybersecurity-statistics>

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ See Bill Toulas, *Ransomware attack on ION Group impacts derivatives trading market*, Bleeping Computer (February 2, 2023), available at <https://www.bleepingcomputer.com/news/security/ransomware-attack-on-ion-group-impacts-derivatives-trading-market/>

Better Markets has recognized the critical nature of these incidents and the broader implications for market stability and integrity.¹⁷ Because of the growing threat landscape, including incidents like the ION Markets attack, Better Markets has advocated for the CFTC to provide a formal rulemaking that provides a cyber resilience framework.¹⁸ Recognizing the distinct nature of these risks and the importance of fostering robust cybersecurity measures within the financial sector, the CFTC proposes a rulemaking to enhance operational resilience for SDs and FCMs.

The Proposed Rule is an important step in developing adaptable and responsive cybersecurity protocols that align with the dynamic nature of cyber risks. This framework emphasizes the need for flexible regulatory measures that can evolve in response to emerging threats, ensuring the derivatives market's protection against the changing landscape of cyberattacks. Moreover, the interconnected nature of financial markets necessitates a collaborative approach among regulatory bodies. With swap dealers often subject to prudential regulation, the CFTC must coordinate with banking agencies to harmonize cybersecurity regulations. This collaboration is vital to address potential regulatory discrepancies and establish a cohesive and comprehensive cybersecurity strategy across the financial industry.

I. The Proposed Rule represents an important advancement in crafting a flexible and proactive operational resilience framework that is in sync with the ever-changing nature of operational threats.

Better Markets acknowledges the CFTC for proposing a rule that requires the establishment of an operational resilience framework for FCMs and swap entities. This proposal is designed to systematically identify, monitor, manage, and assess the myriad of risks associated with information and technology security, third-party relationships, and significant disruptions to normal operations. By integrating principles-based directives with specific minimum requirements, the Proposed Rule ensures a balanced approach that fosters annual risk assessments, stringent information and technology security controls, and diligent monitoring of third-party service providers. The overarching governance, training, testing, and recordkeeping requirements are set to reinforce the ORF's structure, underpinning the holistic objective of operational resilience. Additionally, the proposal includes mandatory notifications to the CFTC and, in certain scenarios, to customers or counterparties, enhancing the transparency and accountability of the operational resilience measures.

¹⁷ See Better Markets, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, available at https://bettermarkets.org/wp-content/uploads/2022/05/Better_Markets_Comment_Letter_Cybersecurity_Risk_Management_Strategy_Governance.pdf, see also Better Markets, Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, available at https://bettermarkets.org/wp-content/uploads/2023/06/Better_Markets_Comment_Letter_SEC_Regulation_SP.pdf

¹⁸ See Better Markets, Risk Management Program Regulations for Swap Dealers, Major Swap Participants, and Futures Commission Merchants, available at https://bettermarkets.org/wp-content/uploads/2023/09/Better_Markets_Comment_Letter_Risk_Management_Program_Regulations_Swap_Dealers_Swap_Participants_Futures_Commission_Merchants.pdf.

The Proposed Rule aligns with the White House's March 2023 National Cybersecurity Strategy, which calls for leveraging established standards and fostering a harmonized regulatory environment that remains agile in response to the technological threat landscape's evolution.¹⁹ This proposal draws on the CFTC's prior experiences and aligns with the standards and practices of both national and international regulatory bodies. Additionally, the Commission engaged with the National Institute of Standards and Technology (NIST) to review standards developed under Executive Order 13636, aimed at reducing cyber risks to critical infrastructure through voluntary consensus standards and industry best practices, ensuring a comprehensive and unified approach to enhancing the financial sector's operational resilience.²⁰

A. Standard

Better Markets appreciates the CFTC's effort in proposing a rule that necessitates FCMs and SDs to adopt an operational resilience framework, integrating "generally accepted standards and best practices."²¹ However, the proposed rule's broad reference to these standards, including those from NIST, International Organization for Standardization, Center for Internet Security, and Federal Financial Institutions Examination Council, without specifying a definitive scope or definition, could lead to inconsistencies in interpretation and application. Given the complexity and variability of cyber threats and the evolving nature of technology, it is crucial for the CFTC to provide more precise guidance on what constitutes these "generally accepted standards and best practices."

The NIST Cybersecurity Framework (NIST CSF), recognized and utilized globally, offers a comprehensive and flexible structure for managing cybersecurity risks, which could serve as a benchmark for the CFTC's ORF requirements.²² The NIST CSF is extensively adopted across various sectors in the U.S. due to its well-established guidelines and practices for combating cyber threats and enhancing operational resilience.²³ It is respected as a best practice in the industry, offering an exhaustive and detailed set of controls within its framework, and is considered the gold standard in cybersecurity frameworks.²⁴

Therefore, Better Markets advocates that the CFTC should explicitly align the ORF's standards with the NIST CSF, ensuring a consistent and robust approach to cybersecurity across the financial sector. This alignment should be explicit in its expectations for FCMs and SDs, thereby ensuring the holistic integration of cybersecurity efforts throughout the industry and

¹⁹ The White House, National Cybersecurity Strategy (Mar. 2023) (National Cyber Strategy), available at <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>.

²⁰ See Proposed Rule at 4710.

²¹ See Proposed Rule at 4712.

²² See Ethan Bresnahan, *What Are the Benefits of the NIST Cybersecurity Framework*, CyberSaint Security, available at <https://www.cybersaint.io/blog/benefits-of-nist-cybersecurity-framework>.

²³ *Id.*

²⁴ See Maria Catricala, *What is the NIST Cybersecurity Framework*, Quick Intelligence (September 24, 2021), available at <https://www.quickintel.com/blog/what-is-the-nist-cybersecurity-framework-csf>.

enhancing the security and resilience of the financial market infrastructure. Importantly, Better Markets emphasizes the necessity for the CFTC to prevent FCMs and SDs from defaulting to a less rigorous framework that may lead to fewer standards. Given the paramount importance of robust cybersecurity defenses, it is critical that all SDs and FCMs adhere to the highest possible standards, such as those offered by the NIST CSF, to safeguard the integrity of the U.S. financial system.

B. Information and Technology Security Program

Better Markets acknowledges the Proposed Rule's inclusion of an information and technology security program within the ORF for FCMs and SDs.²⁵ This initiative is vital for managing the cybersecurity and technological risks in today's rapidly evolving threat environment.

The proposed rule's detailed approach to defining 'information and technology security,' 'covered information,' and 'covered technology' is commendable for its depth, focusing on the preservation of data integrity and system resilience.²⁶ This initiative is critical for protecting essential data and maintaining the confidentiality vital for the security of customers and the broader market. Better Markets supports the rule's focus on risk assessment, control implementation, and incident response planning, as these are key to comprehensively managing cybersecurity risks.

However, Better Markets recommends that the CFTC further refine these definitions and provide more explicit requirements on implementing 'generally accepted standards and best practices.'²⁷ This clarification will prevent potential inconsistencies and ensure uniform application across entities. Additionally, considering the dynamic nature of cyber threats, we urge the CFTC to periodically update these standards to keep pace with technological advancements and emerging threats, thus maintaining the efficacy of the ORF in bolstering operational resilience.

On the operational front, Better Markets supports the requirement that senior leadership within FCMs and SDs certify and approve risk assessments.²⁸ This action will guarantee their active involvement in risk management, aligning with the entities' strategic goals and risk appetites. Given the rapidly evolving cyber threat landscape, we advocate for more frequent, ideally biannual, risk assessments to accurately reflect and quickly adapt to current and emerging threats.

Better Markets also agrees with the necessity of mandating essential cybersecurity controls, like multifactor authentication (MFA), firewalls, and antivirus software, recognized for their effectiveness in strengthening cybersecurity defenses.²⁹ Furthermore, we believe that Chief

²⁵ See Proposed Rule at 4716.

²⁶ *Id.*

²⁷ See Proposed Rule at 4718.

²⁸ *Id.*

²⁹ See Proposed Rule at 4721.

Compliance Officers (CCOs) should be promptly informed of all incidents to ensure they play a significant role in the incident response and remediation processes.³⁰

Better Markets urges the CFTC to integrate these considerations into the ORF to fortify the resilience, responsiveness, and accountability of the framework, thus ensuring the ongoing integrity and stability of the financial markets.

C. Third Party Relationship Program

Better Markets recognizes the CFTC's effort to integrate a third-party relationship program within the proposed ORF.³¹ This program is crucial for managing the complexities and risks associated with FCMs' and SDs' increasing reliance on third-party services, which range from information technology to risk management functions.

While the potential for reduced operating costs and enhanced technological capabilities through third-party services is acknowledged, the risks, as exemplified by incidents like the ION disruption, cannot be ignored. These risks can significantly affect not only individual firms but also the financial system at large. Better Markets supports the CFTC's view that FCMs and SDs must have robust mechanisms to identify, monitor, manage, and assess these risks.

Better Markets appreciates the proposed rule's flexibility, allowing FCMs and SDs to tailor their third-party relationship programs based on the nature and complexity of their third-party interactions. However, we recommend that the CFTC require these entities to periodically review and, if necessary, recalibrate their third-party relationship management strategies, especially for critical service providers whose disruption could significantly impact operations or regulatory compliance.

The proposal to have FCMs and SDs maintain an inventory of third-party service providers, categorizing them based on their level of critical service, is a step in the right direction.³² This will not only aid in risk management but also ensure a strategic approach to monitoring and engaging with these providers. Better Markets believes that such inventories should be regularly updated and reviewed to accurately reflect the current risk landscape.

Furthermore, Better Markets agrees with the proposed rule's stance that FCMs and SDs should retain ultimate responsibility for meeting their regulatory obligations, irrespective of their reliance on third-party services.³³ This accountability is paramount to maintaining the integrity and resilience of the financial system.

While Better Markets supports the CFTC's initiative to address third-party risks within the ORF, we recommend that the Commission consider our suggestions in order to strengthen these

³⁰ *Id.*

³¹ *See* Proposed Rule at 4721.

³² *See* Proposed Rule at 4723.

³³ *Id.*

requirements to ensure that FCMs and SDs are equipped to manage and mitigate the potential risks arising from their third-party relationships effectively.

D. Business Continuity Disaster Recovery Plan

Better Markets supports the proposed rule's introduction of a robust Business Continuity and Disaster Recovery (BCDR) plan as a fundamental component of the ORF, acknowledging its crucial role in mitigating the impact of emergencies or significant disruptions on FCM's and SD's operations.³⁴ The requirement for such a plan aligns with the operational realities that not all disruptions can be prevented or immediately resolved, necessitating strategic and actionable plans to minimize operational impact.

The proposed BCDR plan's scope, extending beyond the incident response plan, signifies a comprehensive approach to operational resilience. Better Markets appreciates the CFTC's efforts to define and streamline the BCDR plan requirements, facilitating alignment with the broader ORF objectives. The focus on ensuring minimal disruption to operations, customers, and counterparties, and the emphasis on recovering and utilizing all necessary information, underscore the plan's importance in maintaining market integrity.³⁵

Better Markets understands the CFTC's rationale to remove the "next business day" standard due to the complexities and varied nature of potential disruptions. However, the CFTC should provide a clear requirement that mandates prompt action, perhaps through language stipulating that recovery efforts should begin "as soon as possible." This would ensure that, despite the removal of a rigid timeframe, there remains a strong imperative for a swift and decisive response to operational disruptions, emphasizing the importance of rapid recovery to uphold market stability and maintain customer trust.

Furthermore, Better Markets sees value in the CFTC's consideration of more specific guidance on transferring business to another entity in emergency scenarios. Such provisions could enhance the financial system's overall resilience by ensuring continuity of operations under adverse conditions.³⁶ The CFTC should maintain a rigorous approach in finalizing the BCDR plan requirements within the ORF, ensuring that FCMs and SDs are well-prepared to handle and recover from disruptions effectively, thereby safeguarding the broader financial ecosystem.

E. Cross-Border Application for Swap Entities

Better Markets vehemently opposes the CFTC's approach to substituted compliance within its cross-border application framework, particularly regarding the proposed extension of regulation 23.603.³⁷ We believe that allowing foreign firms to meet U.S. regulatory standards through

³⁴ See Proposed Rule at 4725.

³⁵ See Proposed Rule at 4726.

³⁶ See Proposed Rule at 4727.

³⁷ See Proposed Rule at 4734.

substituted compliance, especially in the critical area of operational resilience, is fundamentally flawed and undermines the integrity of U.S. financial market regulations.


The importance of a robust Operational Resilience Framework (ORF) has been clearly articulated, emphasizing the need for stringent and enforceable standards to safeguard the financial system against a wide range of risks. The proposed broadening of regulation 23.603 to include comprehensive ORF requirements underscores the necessity for rigorous and direct regulatory oversight.

Better Markets insists that the CFTC should not permit substituted compliance for these expanded regulations. Such a stance would not only compromise the effectiveness of the ORF but also risk the stability and security of the U.S. financial markets. Furthermore, Better Markets strongly urges the CFTC to re-evaluate its entire substituted compliance framework to ensure that it does not inadvertently weaken the regulatory safeguards meant to protect the U.S. financial system.

CONCLUSION

We hope these comments are helpful as the Commission finalizes its Proposed Rule.

Sincerely,

A handwritten signature in black ink, appearing to read "Cantrell Dumas". The signature is fluid and cursive, with the first name being the most prominent.

Cantrell Dumas
Director of Derivatives Policy

Better Markets, Inc.
2000 Pennsylvania Avenue, NW
Suite 4008
Washington, DC 20006
(202) 618-6464
cdumas@bettermarkets.org
<http://www.bettermarkets.org>