By Electronic Submission

September 18, 2023

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

Re: Risk Management Program Regulations for Swap Dealers, Major Swap Participants, and Futures Commission Merchants (RIN 3038-AE59)

Dear Mr. Kirkpatrick:

Better Markets[1] appreciates the opportunity to comment on the advance notice of proposed rulemaking ("ANPRM") issued by the Commodity Futures Trading Commission ("CFTC" or "Commission"), which seeks public comment regarding potential regulatory amendments under the Commodity Exchange Act governing the risk management programs of swap dealers, major swap participants, and futures commission merchants ("FCMs").[2]

Effective risk management is crucial for swap dealers and FCMs as it ensures the stability and integrity of financial markets. Beyond preserving their own financial well-being, prudent risk management serves as a linchpin for bolstering overall market confidence and resilience. By preemptively identifying and mitigating potential risks, these financial entities not only contribute to the seamless operation of markets but also mitigate the risk of financial crises while safeguarding the interests of customers and market participants. Swap dealers and FCMs, as intermediaries in complex financial transactions, are uniquely positioned to influence market dynamics. By meticulously assessing, quantifying, and addressing risks, they preemptively avert scenarios that could undermine market stability.

Nevertheless, recent years have ushered in a new era marked by unprecedented challenges, where the need for evolving risk management practices has never been more apparent. These challenges include the rapid evolution and adoption of emerging technologies, including cryptocurrency and artificial intelligence. These technological advancements bring their own set

---

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 Risk Management Program Regulations for Swap Dealers, Major Swap Participants, and Futures Commission Merchants; 88 Fed. Reg. 45,826 (July 18, 2023).

of risks and uncertainties to the financial industry, further complicating an already intricate risk management environment. Additionally, there has been a string of record-breaking climate-related disasters that have inflicted unprecedented financial losses, highlighting the need to integrate climate risk management into the broader risk mitigation framework of financial entities. Furthermore, there has been a sharp increase in cyberattacks, posing a growing threat to financial institutions and exacerbating the complexity of risk management in the digital age. What further complicates this landscape is the enduring global pandemic, which continues to disrupt supply chains and economic stability.

Better Markets respectfully urges the Commission in its rulemaking to prioritize the alignment of risk management programs for swap dealers and FCMs with the dynamic evolution of financial stability risk. Furthermore, we emphasize the importance of adopting a proactive approach to ensure that these risk management frameworks remain well-prepared to identify and respond to emerging and evolving risks. Such vigilance is essential to safeguarding the integrity and resilience of the financial markets and protecting the interests of market participants and the public.

Below are the following risks that Better Markets strongly asserts the Commission must comprehensively address within its forthcoming risk management rulemaking framework for swap dealers and FCMs.

CLIMATE RISK

Climate change has garnered international and U.S. recognition as a significant threat to both the stability of financial institutions, such as banks, and the broader financial system's overall stability. This recognition is widespread, acknowledged not only by regulatory authorities but also by global organizations.[3] Central banks in countries like Japan, the United Kingdom, France, Germany, the Netherlands, and the United States, and international entities such as the U.S. Financial Stability Oversight Council, the Bank for International Settlements, and the Financial Stability Board, have all underlined the importance of addressing climate risks.[4]

Given the broad acknowledgment of these risks and their undeniable materiality, it is paramount that climate risks become an integral component of the risk management and governance practices employed by swap dealers and FCMs. Moreover, the assessment of these risks should be a fundamental part of the Commission's regulatory evaluation process. An essential aspect of this integration is the inclusion of climate risks within regulatory guidance.

This is imperative given the financial losses stemming from climate events are both substantial and on the rise. In 2022, the U.S. experienced 18 separate weather and climate disasters

---

3 *See* Better Markets' Comment Letter, Principles for Climate-Related Financial Risk Management for Large Financial Institutions (February 6, 2023), available at https://bettermarkets.org/wp-content/uploads/2023/02/Better_Markets_Comment_Letter_Climate_Related_Financial_Risk_Management_For_Large_Financial_Institutions.pdf

4 *Id*.

costing at least $1 billion each, resulting in more than $165 billion in losses – in just one year. This puts 2022 into a three-way tie with 2017 and 2011 for the third-highest number of billion-dollar disasters in a calendar year, behind the 22 events in 2020 and the 20 events in 2021.[5]

The financial damages from disasters in 2022 of $165.1 billion were primarily driven by Hurricane Ian with $112.9 billion in damages, followed by the drought and heat wave that affected the western region of the U.S. and caused more than $20 billion in damages. In aggregate, billion-dollar disaster losses in the last 10 years (2013-2022) reached $1.1 trillion in the U.S. Importantly, these are conservative loss estimates that do not come close to reflecting all the damage from climate events because they only include disasters with more than $1 billion in damages.[6] Disasters below $1 billion in damage still result in significant costs and losses to a local area and should not be overlooked. Such smaller disasters cause damage to residential property, commercial property, agriculture, small businesses, and local infrastructure.

Transition risks have gained prominence and urgency due to the increasing visibility of climate change's physical risks in recent years, a development that was not as evident in the past. Better Markets acknowledges that comprehending climate-related financial risks poses a complex challenge particularly for swap dealers and FCMs, given that the Commission is in the early phases of grasping the nuances of these risks, as well as how to assess and chart their influence on entities regulated by the CFTC.[7] Nevertheless, swap dealers may be affected by climate-related risks in the following ways:

1. Exposure to Climate-Linked Assets: Swap dealers may have investments or exposure to assets, such as bonds or loans, tied to companies or industries vulnerable to climate risks. For instance, if they hold bonds from a fossil fuel company that faces financial challenges due to increasing regulations or a shift in consumer preferences towards cleaner energy sources, they may incur losses.

2. Counterparty Risk: Climate change can impact the creditworthiness of entities. Swap dealers may have counterparty risk with businesses that suffer financial distress due to climate-related factors, leading to potential credit losses.

3. Market Risk: Climate events can disrupt financial markets. For example, extreme weather events may lead to market closures, increased volatility, or reduced liquidity, impacting the valuation of derivatives and the ability to hedge positions effectively.

---

5 *See* Better Markets' Special Report, The Unseen Banking Crisis Concealed Behind the Climate Crisis (August 23, 2023), *available at* https://bettermarkets.org/wp-content/uploads/2023/08/BetterMarkets_Report_Unseen_Banking_Crisis_Behind_Climate_Crisis_08-23-2023.pdf

6 *Id*.

7 *See* Request for Information on Climate-Related Financial Risk, 87 Fed. Reg. 34,856 (June 8, 2022), available at https://www.cftc.gov/sites/default/files/2022/06/2022-12302a.pdf.

4. Operational Risk: Physical disruptions caused by climate events (e.g., floods, hurricanes, or wildfires) can disrupt swap dealers' operations, affecting their ability to execute trades, manage risk, or provide services to clients.

5. Legal Risk: As climate-related litigation increases, swap dealers could face legal risks related to their involvement with clients or investments impacted by climate change.

Against this backdrop, it is important for the Commission to incorporate climate risks into existing risk categories to allow for comprehensive risk management of climate-related financial risks. By integrating climate-related financial risks within the framework of existing risk management policies, procedures, and programs, the Commission can ensure consistent, streamlined, and effective monitoring, management, identification, and reporting of these critical risks. This approach should strike a balance, being both broad in its flexibility and prescriptive in its effectiveness. Climate risks are multifaceted and constantly evolving, requiring a flexible regulatory framework that can adapt to new developments and unforeseen challenges. A principal-based approach allows the Commission to provide general guiding principles, which swap dealers and FCMs can then tailor to their specific circumstances. This adaptability is crucial, given the diverse nature of financial institutions and their unique risk profiles.

However, to ensure that climate risk management remains effective and not merely symbolic, the Commission must provide clear and specific guidance within this principal-based framework. Prescriptive elements should outline the essential steps and criteria that swap dealers and FCMs must follow in assessing, mitigating, and disclosing climate risks. By doing so, the Commission can strike the right balance between flexibility and effectiveness, ensuring that all market participants adhere to a common set of standards while allowing for adaptability to individual circumstances.

This principal-based approach offers several advantages. It accommodates the dynamic nature of climate risks, encourages innovation in risk management practices, and fosters a proactive response to emerging threats. Furthermore, it aligns with the global consensus on addressing climate risks, as recognized by leading international regulatory authorities and organizations. By embracing this approach, the Commission can lead the way in establishing a resilient and forward-looking financial system capable of addressing the challenges posed by climate change effectively.

TECHNOLOGY RISKS

Similar to climate risks, technological risks pose a significant and evolving challenge for swap dealers and FCMs. Better Markets encourages the Commission to include technology risk as a distinct and enumerated listed risk category for swap dealers, akin to the way it is specifically outlined for FCMs. This is due to the rapid advancement and integration of emerging technologies, such as cryptocurrencies and artificial intelligence, which have introduced their own set of complexities and vulnerabilities to the financial industry. Cryptocurrency is a prime example of a technology risk that needs to be accounted for.

In May 2022, TerraUSD-Classic (USTC), ranked as the third largest stablecoin, experienced a devastating loss of its dollar peg, resulting in the obliteration of approximately $500 billion within the cryptocurrency market. This turmoil had a ripple effect across the crypto landscape, causing Bitcoin, the barometer of crypto health, to plunge from its lofty heights of around $68,000 to a level below $20,000. The abrupt suspension of withdrawals by several global crypto lenders, including Celsius, further exacerbated the situation, with Terra's fall viewed as the initial domino in what would become known as the onset of a 'crypto winter.[8]

Adding to the turmoil, FTX, one of the world's largest cryptocurrency exchanges valued at $32 billion, faced an overnight collapse due to fraudulent activities perpetrated by its CEO. The suspension of investor withdrawals triggered a cascade of repercussions, leading to the insolvency of other trading firms with investments tied to FTX, such as BlockFi and Voyager. Additionally, prominent venture capital funds like BlackRock and Sequoia were forced to make substantial write-offs in the wake of this catastrophic event.[9]

In late 2022, both Silvergate Bank and Signature Bank faced dire consequences stemming from their significant involvement in the volatile cryptocurrency markets. Silvergate Bank, following the collapse of the digital asset exchange FTX, attempted to downplay its exposure by stating that it held $11.9 billion in digital asset-related deposits, with FTX accounting for less than 10 percent. However, during the fourth quarter of 2022, Silvergate Bank experienced a severe outflow of digital asset-related deposits, resulting in a staggering 68 percent reduction from $11.9 billion to $3.8 billion. In a bid to cover these deposit withdrawals, the bank resorted to selling debt securities, ultimately incurring a substantial net earnings loss of $1 billion.[10]

The situation worsened as on March 1, 2023, Silvergate Bank announced a delay in releasing its 2022 financial statements, citing deep concerns about its ability to operate as a going concern. This announcement triggered a sharp drop in the bank's stock price, leading to further distress. Subsequently, on March 8, 2023, Silvergate Bank unveiled its plan for self-liquidation, marking a significant fallout due to its extensive involvement in the cryptocurrency market.

Similarly, Signature Bank, which had also heavily concentrated its business model on the digital asset industry, experienced significant setbacks during the second and third quarters of 2022. The bank witnessed deposit withdrawals and a subsequent decline in its stock price, directly linked to disruptions in the digital asset market brought about by the failures of several high-profile digital asset companies. These events serve as stark reminders of the inherent risks associated with

---

8 *See* Akanksha Jalan, Raman Matkovskyy, Systemic risks in the cryptocurrency market: Evidence from the FTX collapse (May 2023), available at https://www.sciencedirect.com/science/article/abs/pii/S1544612323000442

9 *Id.*

10 *See* Statement of Martin J. Gruenberg, ‘‘Recent Bank Failures and the Federal Regulatory Response’’ before the Committee of Banking, Housing and Urban Affairs, U.S. Senate (Mar. 28, 2023), *available at* https://www.banking.senate.gov/imo/media/doc/Gruenberg%20Testimony%203-28-23.pdf

the cryptocurrency markets and the potential ramifications for financial institutions with extensive exposure to this volatile sector.[11]

In addition to the risks linked to cryptocurrencies, the widespread adoption of AI-driven algorithmic trading automation poses a range of threats, including the potential for systemic disruptions.[12] These risks are not only disruptive but also have the capacity to lead to significant financial losses and destabilize market stability. Acknowledging the transformative influence of these technologies on the financial landscape, it is imperative for the Commission to integrate a comprehensive and flexible framework to address these risks within the risk management programs of swap dealers and FCMs.

To this end, Better Markets strongly encourages the CFTC to adopt a principal-based approach similar to that recommended for climate risks. This approach should allow for flexibility in adapting to the rapidly evolving technological landscape, capturing emerging technologies while providing essential guidance and standards that ensure a robust response to these risks.

Within this framework, the Commission should emphasize the importance of comprehensive measures to understand, monitor, and mitigate the unique risks posed by emerging technologies in trading and financial operations. Clear disclosure and reporting requirements can enhance transparency and allow regulators to assess the effectiveness of risk management practices employed by swap dealers in this context.

By addressing technological risks in a forward-looking and adaptive manner, the Commission can help safeguard the financial system against disruptions, bolster market stability, and ensure the continued trust and confidence of market participants. A principled yet flexible approach is key to effectively managing the evolving landscape of technological risks within the financial industry.

CYBERSECURITY RISKS

Cybersecurity risk is typically encompassed within the broader framework of technology risk. However, Better Markets urges the Commission to designate cybersecurity as a distinct and separately enumerated risk management requirement for swap dealers and FCMs.

Speaking on the topic of cybersecurity in 2012, former Federal Bureau of Investigation Director Robert Mueller said "there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been

---

11 *Id.*

12 See Better Markets' Comment Letter, Exemption for Certain Exchange Members (September 27, 2022), available at https://bettermarkets.org/wp-content/uploads/2022/09/Better_Markets_Comment_Letter_Exemptions_for_Certain_Exchange_Members.pdf

hacked and will be hacked again."[13] The former FBI Director's words are just as true now, if not more so, than they were back in 2012. While technology has revolutionized the way corporations conduct business, it has not come without its own set of risks and vulnerabilities. A 2019 survey of cybersecurity professionals reinforces the former FBI Director's statement, with almost half of respondents reporting an increase in cyberattacks on their organization and 79 percent reporting they expect to experience a cyberattack next year.[14] The question of whether or not a company will experience a cyberattack is becoming less a matter of "if" it will happen and more of a matter of "when" it will happen and how much damage will it cause.

The rise in the sheer number of cyberattacks and their growing sophistication has led many to acknowledge cybersecurity threats as one of the top risks facing the private sector. In the World Economic Forum's 2019 Global Risks Perception Survey, respondents cited cyberattacks and data fraud or theft as two of the top five global risks.[15] This is in stark contrast with the results from the same survey conducted ten years earlier, which mentioned neither cyberattacks nor data fraud among the top five global risks. To help put the perceived risks surrounding cybersecurity into context with other risks posed to companies, the PricewaterhouseCoopers' 2022 Annual Global CEO Survey found that cybersecurity edged out the COVID-19 global health crisis as the threat CEOs are most worried about over the next 12 months.[16] That point bears repeating—CEOs viewed the potential threat of a cyberattack or data breach to be a greater threat to their company in 2022 than the risk posed by a global pandemic, a pandemic that has unfolded over several years and exacted a huge toll in human life and economic damage.

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.[17] In addition, malware and ransomware attacks increased in 2020 by 358% and 435%, respectively, from the previous year.[18] 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

---

13 Robert S. Mueller, Director, FBI, RSA Cyber Security Conference (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

14 Press Release, Information Systems Audit and Control Association, New Study Reveals Cybercrime May Be Widely Underreported – Even When Laws Mandate Disclosure (June 3, 2019), New Study Reveals Cybercrime May Be Widely Underreported Even When Laws Mandate Disclosure (isaca.org).

15 World Economic Forum, The Global Risks Report 8 (2019), *available at* https://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.

16 PricewaterhouseCoopers, Reimagining the outcomes that matter (Jan. 17, 2022), *available at* https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2022.html.

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

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

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.[19] 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.[20] This number also does not account for the 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 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 $1million on average.[21] 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.

The financial industry and its participants are not immune or insulated from the growing risk of cyberattacks and data breaches. Why? Securities and Exchange Commission's Chairman Gensler summed it up in a speech last year on cybersecurity and securities law when he cited a quote from the infamous bank robber Willie Sutton when he was asked why he robbed banks: "Because that's where the money is."[22] In fact, the average cost to a financial services company of a cyberattack is 40% higher than the average cost to companies in other sectors.[23] As the financial services 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

---

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

20 *Id.* at 6-7.

21 *Id.* at 6.

22 Gary Gensler, Chairman, Securities Exchange Commission, Cybersecurity and Securities Laws (Jan. 24, 2022) (quoting Federal Bureau of Investigation, "Willie Sutton," https://www.fbi.gov/history/famous-cases/willie-sutton).

23 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. \

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."[24]

To improve cybersecurity resiliency in the financial sector, FSOC recommended that regulators monitor cybersecurity risks through examinations at financial institutions and improve information sharing between private and public sectors, specifically as it relates to cyberattack incident reporting.[25] Federal financial regulators across the federal government have responded by elevating cybersecurity issues to the top of their rulemaking agenda in recent years.[26]

To address the pressing and rapidly evolving cybersecurity challenges facing swap dealers and FCMs, it is crucial for the CFTC to initiate a dedicated rulemaking effort. Recognizing the distinct nature of these risks and the importance of fostering robust cybersecurity measures within the financial sector, Better Markets strongly encourages the Commission to propose a cybersecurity rulemaking for swap dealers and FCMs.

The need for such a rulemaking is underscored by the evolving tactics employed by cybercriminals, who continuously adapt to circumvent existing security measures. As cyberattacks become more sophisticated and persistent, a principled approach that can flexibly adapt to these dynamic threats is essential. A principal-based framework allows for the development of adaptable and responsive cybersecurity measures, ensuring that regulations remain effective in the face of evolving risks.

Moreover, the interconnectedness of financial markets and institutions necessitates a coordinated approach between regulatory agencies. Given that many swap dealers are prudentially regulated, it is imperative for the CFTC to collaborate closely with banking agencies to ensure the harmonization of cybersecurity rules. Such cooperation will help prevent regulatory gaps and ensure a consistent and comprehensive approach to cybersecurity across the financial industry.

In light of the increasing reliance on digital infrastructure and the escalating frequency of cyber threats, cybersecurity has become a cornerstone of financial stability. By proposing a cybersecurity rulemaking tailored to the dynamic challenges posed by cyber threats, the CFTC can take a decisive step in fortifying the resilience of financial institutions. This proactive stance not only strengthens market stability but also instills greater confidence among market participants. In an era where cyberattacks continually adapt and evolve, the Commission's commitment to adaptable and robust cybersecurity measures will prove instrumental in protecting the integrity of swap dealers and FCMs.

---

24 See Financial Stability Oversight Council, Annual Report (2021), *supra* note 7 at 168.

25 *Id.* at 170.

26 *See* Standards for Safeguarding Customer Information, 86 Fed. Reg. 70,272 (Dec. 09, 2021) (to be codified at 16 C.F.R. § 314) (extended Safeguard rules related to data security to non-bank financial institutions); s*ee* Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66,424 (Nov. 23, 2021) (requires banking organizations to notify their primary regulator of a cyber incident within 36 hours).

CONCLUSION

We hope these comments are helpful for the Commission's considerations regarding future risk management program rulemaking.

Sincerely,

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