September 18, 2023

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

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

Dear Secretary Kirkpatrick, Commissioners, and Commission Staff:

Americans for Financial Reform Education Fund and Public Citizen are pleased to submit comments on the Commodity Futures Trading Commission (CFTC or Commission) Advance Notice of Proposed Rulemaking (ANPRM) seeking public comment regarding potential regulatory amendments under the Commodity Exchange Act governing the risk management programs of swap dealers (SDs), major swap participants (MSPs),[1] and futures commission merchants (FCMs).

We thank the Commission for the initiation of risk management requirements through the establishment of risk management programs (RMPs) for FCMs a decade ago,[2] and this request for public comment on any alterations or improvements that should be made to the Commission's risk management and reporting regime.

As the Commission seeks guidance on potential improvements to risk management regulations for swap dealers, it must first revisit its ill-advised 2018 decision to exempt most entities from registering as a swap dealer if their swaps over a 12 month period are less than $8 billion.[3] This absurdly high *de minimis* threshold improperly excuses significant market participants—

[1] Given that there are currently no registered major swap participants (MSPs), for ease of drafting, throughout this comment, any reference to swap dealers (SDs) should be construed to include both SDs and MSPs.
[2] 78 FR at 68506, 14 Nov. 2013. https://www.govinfo.gov/content/pkg/CFR-2015-title17-vol1/pdf/CFR-2015-title17-vol1-sec1-11.pdf
[3] CFTC, "Commission Adopts Permanent $8 Billion De Minimis Exception to the Swap Dealer Definition," 5 Nov. 2018. www.cftc.gov/sites/default/files/2018-11/508/AdoptingRelease_factsheet110518.pdf

including substantial fossil fuel traders like Vitol[4]—from the Commission's risk management regulations.

In addition, the Commission must refrain from granting exemptions to banks (through the issuance of no action letters) from major swap participant risk management regulations. Public Citizen wrote the Commission in 2020 about the controversial exemption extended to Capital One from having to register as a major swap participant after the bank's swaps and other financial arrangements with oil producers caused significant liabilities in its offsetting derivatives contracts when oil markets experienced unprecedented price volatility.[5] Effective risk management requires the Commission to not provide *ad hoc* exemptions from these systemic risk protections.

Recommendations

To reinforce safe and sound practices within the derivatives market based on the most recent information available, the Commission should update RMP regulations in the following ways:

1. Define crypto-asset and climate-related financial risks, specifically enumerate crypto-asset risk, and name climate-related financial risk in the RMP Regulations and require it be incorporated into the identification and management of the enumerated risks;
2. Develop climate risk management guidance for regulated entities that identifies the ways in which climate-related financial risks manifest across all the traditional risks types enumerated in the RMP Regulations, and accordingly requires incorporation into entities' RMPs.
3. Consider extending the Commission's risk management regulations to encompass sizable third-party IT and cloud-service providers that provide order execution, trading, and/or trade processing functions to address cyber risk. The Commission's own Commitment of Trader reports, along with other critical data reporting, left markets completely in the dark for weeks after the ransomware hack of Ion Markets, a key vendor to exchanges and other market participants that was not subject to direct regulatory oversight by the Commission.[6] With key exchanges like CME Group recently signing agreements to shift fundamental derivative clearing operations to cloud servers owned and operated by

[4] Silla Brush, "Swap Regulators Said to Weigh Dealer Threshold of $8 Billion," *Bloomberg*, 11 Apr. 2012. www.bloomberg.com/news/articles/2012-04-11/u-s-swap-regulators-said-to-weigh-dealer-line-above-3-billion

[5] Tyson Slocum, "Public Citizen Urges CFTC to End Exemptions for Banks with Significant Exposure to Oil and Gas Industry," 7 Apr. 2020. www.citizen.org/article/public-citizen-urges-cftc-to-end-exemptions-for-banks-with-significant-exposure-to-oil-and-gas-industry/

[6] Ruth Carson and Stephen Stapczynski, "Frustrated Traders Missing Key Piece of Market Jigsaw Puzzle After London Firm Hacked," *Bloomberg*, 21 Feb. 2023. www.bloomberg.com/news/articles/2023-02-21/frustrated-traders-missing-key-piece-of-market-jigsaw-puzzle

Alphabet,[7] the outsourcing of critical infrastructure to firms outside the Commission's direct regulatory oversight raises risk management vulnerabilities.

4. Question 11 asks whether to require risk exposure reports to detail risk at the registrant level or at the parent corporation level. Given the sprawling and interconnected nature of corporate affiliates, the Commission's risk management regulations must extend to the ultimate parent corporation level to ensure adequate protections from systemic risk.

In addition to these RMP regulatory updates, the Commission should:

- Work with systemically significant regulated entities and its other largest regulated entities on climate scenario analyses to understand current and future climate risks in derivatives markets; and
- Conduct a horizontal supervisory review of climate risk management practices and vulnerabilities at exchanges, clearinghouses, and at market intermediaries.

More details on these recommendations can be found below.

Updating risk management expectations to contend with the modern risk landscape

Risk management is an essential function for all financial institutions, and all financial regulators including the Commission have the responsibility to supervise firms within their remit to ensure adequate and meaningful risk monitoring and management that results in robust firm-level safety and soundness and financial stability. As stated by Commissioner Goldsmith-Romero, "Management of existing, evolving, and emerging risk is paramount to the financial stability of the United States and global markets. This is evidenced by the recent bank failures, followed by subsequent government action taken out of regulatory concern over possible contagion effect to other banks and broader economic spillover."

At present, emerging risks abound, including climate change,[8] cybersecurity,[9] pandemics,[10] and artificial intelligence.[11] These growing threats present significant risk management challenges that firms will need to build capacity for and address quickly with the guidance of regulators.

---

[7] CME Group, "CME Group Signs 10-Year Partnership with Google Cloud to Transform Global Derivatives Markets Through Cloud Adoption," 4 Nov. 2021. www.cmegroup.com/media-room/press-releases/2021/11/04/cme_group_signs_10-yearpartnershipwithgooglecloudtotransformglob.html

[8] FSOC, "Report on Climate-Related Financial Risk," Nov. 2021. https://home.treasury.gov/system/files/261/FSOC-Climate-Report.pdf

[9] Danny Brando et al., "Implications of Cyber Risk for Financial Stability," FEDS Notes, 12 May 2022. https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html

[10] OCC, *Semiannual Risk PErspective for Fall 2021*, Fall 2021. https://www.occ.gov/publications-and-resources/publications/semiannual-risk-perspective/files/semiannual-risk-perspective-fall-2021.html

[11] Lydia Beyoud, "SEC's Gensler Warns AI Risks Financial Stability," *Bloomberg*, 17 July 2023. https://www.bloomberg.com/news/articles/2023-07-17/gensler-warns-artificial-intelligence-risks-financial-stability?

Adding to the urgency, the Spring 2023 banking crisis revealed that financial instability can flow from parts of the financial system and from entities previously thought not to be systemically important and that risk containment is difficult even when dealing with straightforward risks.[12] A precautionary approach is warranted, and regulators should begin by updating their risk management programs, guidance, supervision, and examinations to reflect the new risks facing the financial system and regulated firms, as the Commission begins to consider here.

CRYPTO-ASSET RISKS

As stated by Commissioner Goldsmith-Romero in her statement regarding this notice, "Digital assets carry risks—something that has become all too clear in the past year."[13] These risks are many and varied. And, contrary to the conventional wisdom that blockchain-based platforms provide a greater level of security due to the 'immutability' of distributed ledger technology, these risks are linked to both the technological and economic features of crypto-assets, actors and activities as present in markets today.

Below we offer several examples of such risk, and make recommendations as to how the Commission might better define and explore such risks and update oversight and accountability mechanisms within the context of this rule to enhance risk management mechanisms found both in the crypto-asset sector as well as any regulated entities trading in or exposed to such assets. These are steps that the Commission should be able to take using its existing authority that would help curb significant risks and improve market integrity and stability in the crypto asset industry.

Technological/Platform Risk

Because crypto-assets rely on distributed ledger technology for their creation, issuance, distribution and exchange, it is often assumed that from a technological standpoint, the decentralized nature of these assets and their associated platforms is, if not always predominant (centralized exchanges are a dominant feature of the crypto industry landscape), then certainly nearly always present and intrinsic to their operation. However, there are studies which have called this assumption into question. In July 2022, Trail of Bits, a New York-based firm that provides security assessments and advisory services to major information technology companies,

---

[12] See E.g., Emily Flitter and Rob Copeland, "Silicon Valley Bank Fails After Run on Deposits," *The New York Times*, 10 Mar. 2023. https://www.nytimes.com/2023/03/10/business/silicon-valley-bank-stock.html; Mohamed A. El-Erian, "What Happens in the Banking Sector Won't Stay There," *Bloomberg*, 28 Mar. 2023. https://www.bloomberg.com/opinion/articles/2023-03-28/silicon-valley-bank-fallout-contagion-extends-to-the-economy?; and
Giampaolo Gabbi, "Correlations among risks: Lessons from the Silicon Valley Bank collapse," Centre for Economic Policy Research, 10 July 2023. https://cepr.org/voxeu/columns/correlations-among-risks-lessons-silicon-valley-bank-collapse

[13] 88 FR at 45833, *Appendix 3—Statement of Commissioner Christy Goldsmith Romero on Advance Notice of Proposed Rulemaking on Risk Management Program Regulations*, https://www.federalregister.gov/d/2023-15056/p-165

was engaged by the Defense Advanced Research Project (DARPA) to investigate the extent to which blockchains are truly decentralized. Their study focused on Bitcoin and Ethereum (two of the largest and most popular crypto blockchain platforms).[14]

Their report found that, though the cryptographic tools used to secure blockchain's immutability were often robust (a feature which helps promote decentralization), the platforms they surveyed were vulnerable to exploits or attacks that took advantage of their chain's other properties – their implementation approaches, networks and consensus protocols. A few examples among many:

- Every widely used blockchain has a privileged set of entities that can modify the semantics of a blockchain to potentially change past transactions.
- The number of entities sufficient to disrupt a blockchain is relatively low: four for Bitcoin, two for Ethereum, and less than a dozen for most PoS (Proof of Stake) networks.
- A dense, possibly non-scale free, subnetwork of Bitcoin nodes appears to be largely responsible for reaching consensus and communicating with miners – the vast majority of nodes do not meaningfully contribute to the health of the network.
- Bitcoin traffic is unencrypted - any third party on the network route between nodes (e.g., ISPs, Wi-Fi access point operators, or governments) can observe and choose to drop any messages they wish. Additionally, of all Bitcoin traffic, the researchers found that for extended periods of time, 60% of such traffic traverses just three ISPs.

These vulnerabilities amply demonstrate the technological risks present in crypto-asset markets as result of their unique exposure to risk stemming from internet infrastructure itself; that is, risks that undergird the operation of blockchain platforms, regardless of the code used to create them.

Centralized financial intermediaries may face their own array of risks stemming from the use of information technology, but a key advantage of centralized platforms is the ability for one party to have the means and authority to swiftly and decisively intervene in the face of technological and cybersecurity risks. In contrast, 'decentralized' financial platforms that rely on a distributed network to maintain operations, which in turn rely on cloud computing and other internet based information management systems, will arguably face heightened technological risk in comparison–both because such distributed systems present a 'wider' target, and because their (partially) decentralized nature and the lack of clarity regarding who can or should intervene will impede crypto actors' ability to respond to technological threats.

[14] Trail of Bits, "Are Blockchains Decentralized? Unintended Centralities in Distributed Ledgers," June 2022. https://assets-global.website-files.com/5fd11235b3950c2c1a3b6df4/62af6c641a672b3329b9a480_Unintended_Centralities_in_Distributed_Ledgers.pdf

The Commission should therefore incorporate a definition of technological risk in this rule that recognizes this unique risk scenario. That definition in turn should help the Commission and those entities it regulates to better assess how and whether crypto assets and platforms are able to demonstrate they are able to maintain hardened defenses and resiliency in the face of exposure to such technological risk.

Cybersecurity/Operational Risk

Beyond internet infrastructure, crypto-assets and actors are exposed to or present a number of risks related to the cyber security of these platforms or vulnerabilities stemming from their general operations. To offer some context, much of current crypto derivatives trading activity does not typically occur directly on the blockchain, but on more conventional trading platforms. But the underlying assets for these trades do exist on the blockchain, which means that the cybersecurity risks found there can translate into operational and market risks.

As we briefly discussed above, the rhetoric around blockchain technology often asserts that, at least at its core, the immutability of blockchain protocols somehow provides, or will provide, a higher level of security for financial platforms than currently exists with traditional finance. The current reality is often far different. Like any software program or computer network, crypto platforms are just as vulnerable—if not more so—to the cyber security risks faced by more conventional computing tools and programs. A few examples include the following

- The code used to develop crypto assets and platforms can contain bugs or flaws that offer hackers opportunities to breach platforms and steal assets. Sometimes, blockchain developers themselves use code they develop to orchestrate "inside jobs."
- Other times, flaws in code that is meant to be 'self-executing' can execute transactions or activities that end up being harmful to exchange participants, despite participants' best efforts to stop them.
- New layers of code that bypass the layer 1 chains to deal with slow transaction speeds introduce new complexity and vulnerabilities. Bridges created to deal with interoperability challenges have become one of the most vulnerable points.

The Commission should consider updating its rules to include a full and thorough set of criteria to identify and evaluate cybersecurity and operational risks associated with the creation, issuance and trading of crypto-assets. This is especially important given that many in the industry seek to increase reliance on software protocols and automated processes that are meant to displace the role that human or institutional intermediaries play in financial transactions. The Commission has already been presented with petitions to allow such activity to occur, such as the petition presented to the Commission in March 2022 by Ledger X (d/b/a as FTX US Derivatives) to allow direct trading and clearing on its platform.[15] The lessons learned from the FTX collapse

[15] CFTC Press Release, "CFTC Seeks Public Comment on FTX Request for Amended DCO Registration Order," 10 Mar. 2022. https://www.cftc.gov/PressRoom/PressReleases/8499-22

with respect to cybersecurity should offer clear guidance on how to properly weigh the risk of allowing such petitions to proceed without adequate cybersecurity requirements in place.

Affiliate or Counterparty Risk

The degree to which affiliate or counterparty risk is present in crypto markets is well known. The risk and harm incurred by investors as a result of their exposure to FTX's trading partner, Alameda Research, is now well-established[16], but arguably much of the harm and loss that occurred in 2022 was due to poorly understood affiliate risks throughout the industry. Indeed, affiliate or counterparty risk has immediate ramifications for the parties directly involved with trades, but such risk is often linked with broader contagion risks. The collapse of Terra/Luna in May 2022 exposed a series of trades, loans and investments made by other crypto platforms and investors (such as Three Arrows Capital, Voyager, Celsius and many others) that carried significant counterparty risks, ones which were either poorly understood by these platforms (and their customers) or largely disregarded.[17]

These arrangements also demonstrated a high degree of interconnectivity and centralization found throughout crypto markets and platforms. That centralization—rooted in economics and management—has not appeared to change much after the height of the crypto crash. As of January 2023:

- Two mining pools controlled 51% of Bitcoin's hash rate (with similar levels of concentration found on other chains);[18]
- 66.7% of all crypto trading on centralized exchanges (which themselves constitute the bulk of all crypto trading) occurred on Binance[19] (a dynamic that largely holds true today, though Binance has seen changes in trading volume due to investor concerns about ongoing and pending law enforcement actions);[20]
- As of July 2022 one analysis determined that .04% of BTC addresses (or wallets) held 62.25% of all Bitcoins issued;[21] and
- A recent Wall Street Journal article revealed how a group of roughly half a dozen coders "serve as stewards of Bitcoin Core, an open-source program that keeps the

[16] Matthew Goldstein et al., "How FTX's Sister Firm Brought the Crypto Exchange Down," *The New York Times*, 18 Nov. 2022. https://www.nytimes.com/2022/11/18/business/ftx-alameda-ties.html

[17] Nat Rubio-Licht et al., "Everything you need to know about the crypto crash," *Protocol*, 14 July 2022. https://www.protocol.com/fintech/crypto-crash-explainer-blockchain

[18] Andjela Radmilac, "The centralization of Bitcoin: Behind the two mining pools controlling 51% of the global hash rate," *CryptoSlate*, 1 Jan 2023. https://cryptoslate.com/behind-the-two-mining-pools-controlling-51-percent-of-the-global-hash-rate/

[19] Ruholamin Haqshanas, "Binance has Grabbed Two-Thirds of all Crypto Trading Volume – What Happened to the Decentralization of Finance?" *Cryptonews*, 6 Jan. 2023. https://cryptonews.com/news/binance-has-grabbed-two-thirds-of-all-crypto-trading-volume-what-happened-to-the-decentralization-of-finance.htm

[20] Lyllah Ledesma, "Binance's Market Share Fell Further in June," *CoinDesk*, 28 June 2023. https://www.coindesk.com/markets/2023/06/28/binances-market-share-fell-further-in-june/

[21] Francisco Rodrigues, "Hodlers and whales: Who owns the most Bitcoin in 2022?" *Cointelegraph*, 4 July 2022. https://cointelegraph.com/news/hodlers-and-whales-who-owns-the-most-bitcoin-in-2022

> cryptocurrency's digital ledger up-to-date on thousands of computers that make up its network."[22]

This concentration should not be viewed solely as an inevitable feature of economic actors seeking advantage (though that certainly is a contributing factor). Rather, this concentration, with the heightened conflicts of interests such concentration presents, is often the goal. Despite crypto industry assertions that decentralization is desirable, achievable, and the key innovation that crypto-assets offer to the financial sector, many industry business models are vertically integrated, with the platform playing the role of custodian, exchange, market maker and broker all in one. To the extent that such models persist in the crypto environment, without these roles and functions being disaggregated, we believe counterparty risks will continue to be high for those participating in these markets.

Lastly, counterparty risk is also an omnipresent phenomenon in the crypto asset ecosystem in part due to features in the market that obscure the identity or nature of the entities involved in trading. The European Securities and Markets Authority (ESMA), in an October 2022 report analyzing crypto assets and their risks for financial stability, noted that:

> "The *pseudonymity that prevails in crypto-asset markets makes it virtually impossible to assess the creditworthiness or aggregate exposures of participants*. Pseudonymity refers to the string of letters and numbers that constitute the "public keys" of self-custody wallets that often do not require any know-your-customer procedures to be created. Similarly, concentrations of asset holdings are difficult to identify because the same individual or entity may own several pseudonymous wallets (making their total balance impossible to trace). Estimates suggest there is a significant inequality in the distributions of certain assets (i.e. 2 % of wallets possess 94 % of all Bitcoins), which has implications in terms of liquidity but also *market integrity* (i.e. in the case of large orders distorting price formation). More broadly, the current lack of transparency and reliable data to assess exposures and risks is a source of concern for consumer protection, market order and financial stability alike (*emphasis added)*."[23]

The commission should pursue the development of definitions that thoroughly explore counterparty and/or affiliate risk through the crypto-asset ecosystem. Those definitions should explore both direct and indirect relationships, and be crafted to address the challenges presented by pseudonymity as well as those present on decentralized platforms, where the relationships between trading parties and intermediaries can be unclear or contested.

---

[22] Paul Kiernan, "Bitcoin's Future Depends on a Handful of Mysterious Coders," *The Wall Street Journal*, 16 Feb. 2023. https://www.wsj.com/articles/bitcoin-core-maintainers-crypto-7b93804

[23] ESMA, "Crypto Assets and their risks for financial stability," 4 Oct. 2022. https://www.esma.europa.eu/sites/default/files/library/esma50-165-2251_crypto_assets_and_financial_stability.pdf

Custody Risk

The crypto industry has a poor track record when it comes to ensuring investor assets are secure and well protected from loss, theft or misappropriation. The recent and ongoing crash of crypto markets has laid bare widespread problems with respect to custody of crypto investors' assets. FTX's failure and/or willful misappropriation of the assets it custodied for its clients, and the travails of Celsius' investors who may lose their assets in bankruptcy proceedings because Celsius' terms of use failed to provide for segregation of those assets in the event of insolvency, are notable examples. But, these examples, while egregious and significant in scale, are by no means the only examples of custody failures within the crypto industry. We share a few more below to help illustrate how commonplace these failures have been throughout the sector:

- **Vulcan Forged Wallet Hack**: In December 2021, a hacker stole crypto valued at $140 million from Vulcan Forged, a crypto gaming ecosystem that includes its own decentralized crypto exchange, wherein users trade its native token, PYR. Upon registering their accounts, Vulcan Forged customers were given a set of wallets on various blockchains (Ethereum, Polygon and VeChain) that allowed them to use tokens on the platform, which the platform managed for them. The wallets themselves were created by a third party, Venly. The hacker was able to steal 96 private keys (corresponding with a similar number of wallets) from the platform.[24]
- **Crypto.com Wallet Hack:** In January 2022, Singapore-based Crypto.com, a major crypto exchange, experienced a security breach that led to the theft of ETH and BTC, with values at the time approaching as much as $33 million, according to both the platform and industry analysts. The assets were taken from custodial wallets Crypto.com hosted for its customers. The stolen ETH was moved through Tornado, a platform that 'mixes' crypto transactions, making them more difficult to track. At the time of the hack, Crypto.com customers were reporting their losses online, and analysis suggested that the hackers were able to bypass or override the two-factor authentication protocols set up to prevent unauthorized transactions associated with their hosted wallets.[25]
- **Voyager Bankruptcy:** Voyager provided custody services for its clients, who used fiat currency to purchase crypto on Voyager's platform with the intent of receiving a return on their investment. Voyager portrayed themselves as a reputable, reliable company, subject to meaningful oversight: "Publicly traded, licensed and regulated." The firm claimed that their customers' USD 'deposits' were held by its FDIC-insured banking partner, Metropolitan Commercial Bank (MCB) – but neglected to explain that the cash in question was protected in the event MCB failed, not Voyager. We now know Voyager

[24] Tim Copeland, "96 private keys stolen from Vulcan Forged in $140 million theft," *The Block*, 13 Dec. 2021. https://www.theblock.co/post/127270/96-private-keys-stolen-from-vulcan-forged-in-140-million-theft

[25] Osato Avan-Nomayo, "On-chain analyst claims Crypto.com hack was closer to $33 million," *The Block*, 19 Jan. 2022. https://www.theblock.co/post/130793/on-chain-analyst-claims-crypto-com-hack-was-closer-to-33-million; Emily Nicolle, "Crypto.com Suspends Withdrawals After 'Unauthorized Activity'," *Bloomberg*, 17 Jan. 2022. https://www.bloomberg.com/news/articles/2022-01-17/crypto-com-suspends-withdrawls-after-unauthorized-activity?sref=f7rH2jWS

> commingled its customer funds with its own and became over leveraged due to its rehypothecation of customer assets for lending purposes. And, when Voyager went into bankruptcy after the collapse of Three Arrows Capital, due to a loan Voyager made to that firm, many Voyager customers learned that their assets were not protected in the event of bankruptcy and became unsecured creditors overnight. Many Voyager customers have yet to recoup their investments due to prolonged bankruptcy proceedings and have effectively lost tens or hundreds of thousands of dollars' worth of their investments.[26]

Custody of client assets is not an esoteric or marginal aspect of financial management or investment activity. It is core to the role that financial intermediaries play in finance. Investment advisers must ensure the assets they maintain for their clients are protected against theft, loss, misuse or misappropriation, and that in the event of insolvency, they are protected against loss. Moreover, if investors do not have confidence that the funds they've entrusted to investment advisers and custodians are safe from theft or misuse and secure in the event of insolvency, they will be less likely to entrust their assets to others, which will in turn slow the wheels of financial markets overall.

Crypto investors and market participants would benefit from clear, robust rules for crypto custody that would ensure custody options for crypto investors and their advisers are safe, secure and reliable. The standard of care for crypto asset custody should at the very least be consistent with that required for custody of other financial assets maintained by well-regulated and licensed financial intermediaries on behalf of their clients. And, there are today entities that exist which do meet, or may be able to meet, such standards.

The Commission should explore and develop definitions related to crypto-asset custody that encompass the wide range of custody arrangements present with the industry and the risks those arrangements present (from hosted to un-hosted wallets; third-party custody arrangements as well a 'self-custody' via air gapped, 'cold' wallets) to ensure that the ranges of custody present in the market are taken into account when updating regulatory oversight for SDs and FCMs. Above all, the Commission should view with a skeptical eye proposals for custody provision that do not meet the broader financial industry standards, on grounds that crypto custody should be treated 'differently' because of the technological platform upon which such services are offered.

CLIMATE-RELATED FINANCIAL RISKS

[26] Michael Shing, "What in crypto hell just happened to all your money?" *Forkast*, 30 Aug. 2022. https://forkast.news/what-did-voyager-do-with-your-crypto-money/; Dallas G. Taylor, "Charting New (and Familiar) Territory: The Voyager Crypto Bankruptcy," *Mintz*, 18 July 2022. https://www.mintz.com/insights-center/viewpoints/2831/2022-07-18-charting-new-and-familiar-territory-voyager-crypto#:~:text=Much%20like%20a%20traditional%20trading,earn%20interest%20on%20the%20deposit.

Climate change poses a serious threat to the safety and soundness of individual financial institutions and the financial system as a whole.[27] Physical climate-related impacts and the inevitable transition to a low-carbon economy together create market, credit, counterparty, liquidity, operational, and reputational risks[28] and financial authorities believe such climate shocks may be correlated,[29] occur in series and in parallel,[30] and affect many major institutions simultaneously, amplified by network effects.[31] Financial regulators and institutions must deploy a proactive, precautionary approach[32] that recognizes the "radical uncertainty" that climate has injected into the financial system. Improved forecasting, metrics, and governance of climate financial risks will be essential, as will qualitative and narrative approaches to scenario analysis where economic models fall short of capturing the full scale of climate risks.[33]

Incorporating climate-related financial risk into the risk management programs of SDs and FCMs alongside all other risk types is an urgent task that should commence quickly to protect consumers and the financial system. Derivatives markets are designed to help entities hedge or transfer risk exposure, however these markets may fail to function in the face of swift, correlated losses between interconnected firms. The Commission should be evaluating climate risk in the exchange traded derivatives market and the over the counter (OTC) market, paying close attention to the interconnectedness between financial institutions, and monitoring the overall growth of climate risk within the system.

Defining Climate-related Financial Risks (See Question B.7.a)[34]

---

[27] FSOC, "Report on Climate-Related Financial Risk," Nov. 2021. https://home.treasury.gov/system/files/261/FSOC-Climate-Report.pdf

[28] OCC, "Principles for Climate-Related Financial Risk Management for Large Banks," 16 Dec. 2021. https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-138a.pdf

[29] BIS, Basel Committee on Banking Supervision, "Climate-related risk drivers and their transmission channels," Apr. 2021. https://www.bis.org/bcbs/publ/d517.pdf

[30] Viral V. Acharya et al., "Climate Stress Testing," National Bureau of Economic Research, Apr. 2023. https://www.nber.org/papers/w31097

[31] ECB, "System-wide amplification of climate risk," Accessed 18 Sep. 2023. https://www.ecb.europa.eu/pub/financial-stability/macroprudential-bulletin/html/ecb.mpbu202206_2~1bec56088f.en.html

[32] Hugues Chenet et al., "Finance, climate-change and radical uncertainty: Towards a precautionary approach to financial policy," *Ecological Economics*, **183**, May 2021. https://www.sciencedirect.com/science/article/pii/S092180092100015X?via%3Dihub

[33] Lydia DePillis, "Pace of Climate Change Sends Economists Back to Drawing Board," *The New York Times*, 25 Aug. 2022. https://www.nytimes.com/2022/08/25/business/economy/economy-climate-change.html?

[34] 7. Are there any other types of risk that the Commission should consider enumerating in the RMP Regulations as risks required to be monitored and managed by SDs' and FCMs' RMPs? Geopolitical risk? Environmental, social and governance (ESG) risk? Climate-related financial risk, including physical risk and transition risk such as the energy transition? Reputational risk? Funding risk? Collateral risk? Concentration risk? Model risk? Cybersecurity risk? Regulatory and compliance risk arising from conduct in foreign jurisdictions? Contagion risk? a. Should these potential new risks be defined in the RMP Regulations?

The Commission should define "climate-related financial risks" in the updated RMP regulations to include "physical" and "transition" risks. The Commission should make clear to FCMs and SDs that climate risk must be monitored and managed under all of the enumerated risk types.

We propose the following definitions:

> Physical risks: *The actual or potential negative impacts of climate-related conditions and events on a firm's balance sheet, financial statements, operations, or value chains including those resulting from adverse consequences to communities and from chronic risks from longer-term weather patterns and related effects, including but not limited to sustained higher temperatures, sea level rise, drought, and increased wildfires, as well as related effects such as decreased arability of farmland, decreased habitability of land, and systemic threats to public health and safety, such as extreme heat, poor air quality, reduced quantity and quality of food and water, changes to infectious disease vectors, strain on infrastructure, political instability, and population displacement.*

> Transition risks: *The actual or potential negative impacts on a firm's balance sheet, financial statements, operations, or value chains attributable to regulatory, technological, social, and market changes to address the mitigation of, or adaptation to, climate-related risks, such as increased costs attributable to changes in law or policy, reduced market demand for carbon-intensive products leading to decreased prices or profits for such products, the devaluation or abandonment of assets, risk of legal liability and litigation defense costs, competitive pressures associated with the adoption of new technologies, as well as reputational, operational, legal, and political impacts (including those stemming from a firm's customers or business counterparties as well as adverse social conditions such as increasing inequality, land and human rights violations, or shifts in community perceptions of a firm's contribution to or detraction from the transition to a lower-carbon economy) that might trigger changes to market behavior, consumer preferences or behavior, and firm behavior.*

Climate-related Risk to Commodities Futures

Climate change has current and future impacts on commodities and commodity price volatility, and when commodities are affected by significant and unpredictable risks like climate change, this creates volatility in derivatives markets as well.[35] When functioning well, commodity and derivative markets help with price discovery and allow producers and end-users alike to hedge

[35] Todd Phillips, "A Climate and Competition Agenda for the Commodity Futures Trading Commission," *Center for American Progress*. 1 Feb. 2022. https://www.americanprogress.org/article/a-climate-and-competition-agenda-for-the-commodity-futures-trading-commission/; "Climate Change Rocks Agricultural Commodity Market," *Voice of America*. 13 Nov. 2021. https://www.voanews.com/a/climate-change-rocks-agricultural-commodity-market/6310895.html

against price risk. But market participants may not be able to rely on these markets during climate shocks and geopolitical instability that creates pricing volatility or render markets fundamentally dysfunctional.[36]

As has been evident from the COVID-19 pandemic and climate impacts to date, shocks to global and regional supply chains can have rippling effects on markets. The commodities underlying the markets within the Commission's purview–including agriculture, energy, and metal commodities–will likely experience climate shocks that drive significant volatility in the derivative markets.

Along with physical risks and climate shocks, the energy transition may introduce new sources of volatility into commodity markets that the Commission must monitor and help exchanges and market participants prepare for. The adoption of the Inflation Reduction Act (IRA) is likely to accelerate growth in demand for minerals like copper and lithium, which are critical for the clean energy and battery technologies needed at scale for the transition. One example of a related risk is what happened with the nickel market collapse in early 2022: one speculator, a major Chinese producer, anticipated that the price of nickel would fall, only to have the unexpected invasion of Ukraine by Russia (a major nickel exporter) occur, resulting in economic sanctions on Russia and the price of nickel soaring. This led to the London Market Exchange (LME) needing to suspend its contracts and cancel all trades on March 8, 2022.[37] The collapse could have been avoided with effective position limits by the LME.

Such risks are particularly exacerbated in energy markets, which have been subject to numerous sources of volatility over the last decade. Energy market volatility has been especially high since the invasion of Ukraine. Energy traders have pushed the European Central Bank to loosen margin requirements or inject liquidity into markets to allow them to continue taking speculative profits. Meanwhile, the United Kingdom has extended $40 billion in liquidity to energy market participants struggling to make margin calls.[38] In the United States, the IRA's provisions mean that high energy prices overall may trend downward thanks to massive incentives for investment in domestic energy supply, and experts believe the substantial incentives for clean energy in particular will ultimately drive down demand for oil and gas.[39] These rapid changes reinforce the importance of careful oversight by the Commission of its regulated entities and markets to ensure that they are accurately accounting for transition risk along with other sources of energy

[36] Tyson Slocum, "Commodity Futures Trading Commission Letter on Speculation," *Public Citizen*, Mar. 2022. https://www.citizen.org/commodity-futures-trading-commission-letter-on-speculation/
[37] Julia Horowitz, "The broken nickel market is a warning to Wall Street," *Before the Bell at CNN Business*, 17 Mar. 2022. https://www.cnn.com/2022/03/17/investing/premarket-stocks-trading
[38] Javier Blas, "The UK's Cryptic £40 Billion Bailout for Energy Traders," *The Washington Post*. 26 Sep. 2022. https://www.washingtonpost.com/business/energy/the-uks-cryptic-40-billion-bailout-for-energy-traders/2022/09/26/f174be74-3d58-11ed-8c6e-9386bd7cd826_story.html
[39] Princeton University Zero Lab, "Preliminary Report: The Climate and Energy Impacts of the Inflation Reduction Act of 2022," Aug. 2022. https://repeatproject.org/docs/REPEAT_IRA_Prelminary_Report_2022-08-04.pdf

volatility.

Climate-related Risk from Financed Emissions

The Partnership for Carbon Accounting Financials (PCAF)[40]–now in use by over 200 financial institutions worldwide, offers a reliable accounting framework for banks and other financial institutions to calculate and disclose their financed emissions, which are quantitative factors associated with a firm's transition risk. While PCAF has not yet published guidance on emissions associated with derivatives, the Commission should consider offering guidance to SDs and FCMs on how to adjust the PCAF financed emission methodology to treat derivatives as an additional source of debt financing,[41] and then encourage disclosure of these emissions. Firms with public net zero transition commitments should phase down financed emissions from derivatives, and regulators should work with firms to develop credible climate risk management strategies and ensure that firms' public climate commitments are fully aligned with their internal risk management, strategy, and governance across all of their financial arms.

Climate-related Operational Risk and Resilience (See Question B.5)[42]

The Commission should add a definition of "operational risk" to the RMP Regulations that is closely aligned with the Federal Reserve and Basel III's definition of operational risk as "the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events." Adding a definition of "operational risk" should increase clarity for SD and FCM risk management practices, and the Commission should also consider drafting guidance describing major sources of operational risk and appropriate risk management strategies. Specifically, the Commission should consider how physical and transition risk might map on their operational risk exposure for physically settled fossil fuel and critical mineral futures.

RMU Personnel (See Question A4)[43]

The Commission should require that RMU personnel, such as model validators, have experience with climate science or modeling and climate financial risk management[44] experience. The RMU

---

[40] Website for the Partnership for Carbon Accounting Financials, Accessed 18 Sept. 2023. https://carbonaccountingfinancials.com

[41] For recommendations see: Ceres, "Derivatives and Bank Climate Risk: Financing a Net Zero Economy," Sep. 2022. https://www.ceres.org/sites/default/files/reports/2022-09/Ceres%20Derivatives%20and%20Bank%20Climate%20Risk%20Report%202022_0.pdf

[42] B. Enumerated Risks in the Risk Management Program Regulations. 5. The Federal Reserve and Basel III define "operational risk" as the risk of loss resulting from inadequate or failed internal processes, people, and systems or from external events.[44] Would adding a definition of "operational risk" to the RMP Regulations that is closely aligned with this definition increase clarity and/or efficiencies for SD and FCM risk management practices, or otherwise be helpful? Should the Commission consider identifying specific sub-types of operational risk for purposes of the SD and FCM RMP requirements?

[43] A. Risk Management Program Governance. 4. Should the Commission propose and adopt standards for the qualifications of certain RMU personnel (e.g., model validators)?

[44] Elizabeth Langel and Sarah Sliva, "Financial services focus: The emerging role of the climate risk officer," *Heidrick & Struggles*. Accessed 26 June 2023. https://www.heidrick.com/en/insights/financial-services/financial-

personnel should be tasked with, amongst other things, engaging with PCAF, the Network for Greening the Financial System (NGFS), and other international standard setters and industry initiatives to stay up to date on best practices around climate-related financial risk management.

Alignment with Other International and US Regulators (See Question A6)[45]
Consider aligning RMP guidance, as appropriate, with relevant aspects of the "Principles for the effective management and supervision of climate-related financial risks" published by the Basel Committee on Banking Supervision,[46] and harmonizing the Commission's guidance with respect to emerging climate risk with guidance from other financial regulators such as the Federal Reserve, the OCC, and the FDIC.[47]

In addition to updating the RMP guidance to include climate-related financial risk, the Commission should pursue the following actions to better manage and mitigate climate risks in their regulated markets and entities.

Scenario Analysis and Stress Tests
The Commission should incorporate climate-related risks into its stress tests and conduct climate scenario analysis exercises in line with other financial regulators.[48] The Commission regularly conducts supervisory stress tests of central clearinghouses or central counterparties, also known as derivatives clearing organizations (DCOs), to ensure they can handle a range of extreme scenarios. Currently, the tests do not incorporate climate-related considerations, but they should. Stress tests look at whether DCOs have sufficient reserves, whether they are collecting enough margin from their counterparties, and whether they would be able to collect new capital from

---

services-focus-the-emerging-role-of-the-climate-risk-officer; "Fifth Third Appoints Michele Mullins Climate Risk Officer; Role Reflects Bank's Commitment to Managing Climate Change Risk," *Fifth Third Bank*, 24 Sep. 2021. https://www.53.com/content/fifth-third/en/media-center/press-releases/2021/press-release-2021-09-24.html; OCC, "OCC Announces Chief Climate Risk Officer," 12 Sept. 2022. https://www.occ.gov/news-issuances/news-releases/2022/nr-occ-2022-110.html#:~:text=WASHINGTON%E2%80%94The%20Office%20of%20the,%2C%20policy%2C%20and%20external%20engagement.

[45] A. Risk Management Program Governance. 6. Are there other regulatory regimes the Commission should consider in a holistic review of the RMP Regulations? For instance, should the Commission consider harmonizing the RMP Regulations with the risk management regimes of prudential regulators?

[46] BIS, Basel Committee on Banking Supervision, "Principles for the effective management and supervision of climate-related financial risks," June 2022. https://www.bis.org/bcbs/publ/d532.pdf

[47] OCC, "Risk Management: Principles for Climate-Related Financial Risk Management for Large Banks; Request for Feedback," 16 Dec. 2021. https://www.occ.gov/news-issuances/bulletins/2021/bulletin-2021-62.html; FDIC, "Request for Comment on Statement of Principles for Climate-Related Financial Risk Management for Large Financial Institutions," 30 Mar. 2022. https://www.fdic.gov/news/financial-institution-letters/2022/fil22013.html; Federal Reserve Board, "Principles for Climate-Related Financial Risk Management for Large Financial Institutions," 8 Dec. 2022. https://www.federalreserve.gov/newsevents/pressreleases/other20221202b.htm

[48] Board of Governors of the Federal Reserve System, "Press Release: Federal Reserve Board announces that six of the nation's largest banks will participate in a pilot climate scenario analysis exercise designed to enhance the ability of supervisors and firms to measure and manage climate-related financial risks," 29 Sept. 2022. https://www.federalreserve.gov/newsevents/pressreleases/other20220929a.htm

their members if their reserves would not cover their needs.[49] DCOs need to be able to withstand the unique risks climate change presents to their operations and to their largest clearing members.

Climate scenarios ultimately will need to incorporate climate shocks in series and in parallel, rather than as discrete perturbations—the flawed approach the Federal Reserve is currently using—to reflect the potential correlated nature of physical and transition risks. Scenarios should reflect that the worst climate-related floods and fires of the upcoming decades will be far more severe and destructive than the events of the past, as new records are now set regularly. For instance, despite there only being a 0.5% chance forecast of Houston flooding in any given year, it recently experienced a '1-in-500-year' flood event each of three years in a row.[50] During a one month period in the summer of 2022, at least six '1-in-a-1,000-year' rainfalls, each event with only a 0.1% chance of occurring in any given year, damaged cities and regions across the U.S.[51] The National Oceanic and Atmospheric Administration (NOAA) just confirmed that the U.S. has set a record for the most natural disasters in a single year that have cost $1 billion or more.[52] The record-breaking 23 such events in 2023 have occurred with four months remaining in the year.

The Commission should also join the NGFS as a member to access more knowledge on and potentially influence the development of more relevant future climate scenarios and modeling tailored for derivatives markets. Some of this framework for modeling could come from ESMA, which in early 2022 put out its own call for evidence regarding a new climate stress testing framework for central counterparties, which are equivalent to US derivatives clearing organizations.[53] From 2022-2024, ESMA intends to "Develop methods, parameters and scenarios for bottom-up climate change stress testing to be used by supervisors and supervised entities," which it will do in coordination with the European Banking Authority and the European Insurance and Occupational Pensions Authority. ESMA also plans to perform regular

[49] Todd Phillips, "A Climate and Competition Agenda for the Commodity Futures Trading Commission," *Center for American Progress*. 1 Feb. 2022. https://www.americanprogress.org/article/a-climate-and-competition-agenda-for-the-commodity-futures-trading-commission/

[50] "Houston is experiencing its third '500-year' flood in 3 years. How is that possible?" *The Washington Post*, 2017. https://www.washingtonpost.com/news/wonk/wp/2017/08/29/houston-is-experiencing-its-third-500-year-flood-in-3-years-how-is-that-possible/

[51] Scott Sistek, "6 rare '1,000-year' rain events within a month? Climate change may force NOAA to update criteria," *FOX Weather*, 24 Aug. 2022. https://www.foxweather.com/extreme-weather/5-rare-1000-year-rain-events-within-a-month-climate-change-may-force-noaa-to-update-criteria

[52] NOAA, "Billion-Dollar Weather and Climate Disasters," Accessed 18 Sep. 2023. https://www.ncei.noaa.gov/access/billions/#:~:text=In%202023%20(as%20of%20August,and%201%20winter%20storm%20event.

[53] David Clarke, "US regulator considers climate stress tests for commodities and derivatives markets," *Green Central Banking*, 7 June 2022. https://greencentralbanking.com/2022/06/07/climate-stress-tests-commodities-derivatives/; ESMA, "ESMA Launches Call for Evidence on Climate Risk Stress Testing for CCPS," 23 Feb. 2022. https://www.esma.europa.eu/press-news/esma-news/esma-launches-call-evidence-climate-risk-stress-testing-ccps

climate change stress tests or scenario analyses on its regulated entities.[54]

Margin Requirements

The Commission should encourage central counterparties and exchanges to raise margin requirements to account for rising climate risk to protect counterparties and exchanges in the event that derivatives bets go sour by keeping sufficient cash on the table, keeping trading platforms solvent, and preventing contagion. Even when effective capital requirements are established, margin requirements are necessary to ensure that individual commodity products and markets are protected from climate risk.

Exchanges set significantly higher margins for products perceived as risky. For example, the Chicago Mercantile Exchange (CME) set the initial margin for bitcoin futures at 25-30% of notional value, well above the typical 3-12% of notional value for futures contracts, because of the volatility and risks in that market.[55] After turmoil in the West Texas Intermediate (WTI) crude oil contract (which saw a one-day price fluctuation of $55 to a first-ever dive into negative pricing), CME raised crude oil futures maintenance margins by 20% in June 2020.[56] Increased margin requirements reflect increased risk, and carbon-intensive products–such as fossil fuel derivatives–have heightened transition risk that should be reflected in margin requirements.

CONCLUSION

We thank the Commission for recognizing the need to periodically evaluate existing oversight and regulations, and for issuing this ANPRM as the first step toward addressing the emerging risk disclosure and management needs of all market participants in light of new challenges brought on by climate change, crypto-assets, and cybersecurity threats, among other risks. For more information, please reach out to Jessica Garcia (jessica@ourfinancialsecurity.org) and Alex Martin (alex@ourfinancialsecurity.org) on climate risks, to Mark Hays (mark@ourfinancialsecurity.org) on crypto-asset risks, and to Tyson Slocum (tslocum@citizen.org) on cybersecurity threats.

Sincerely,
Americans for Financial Reform Education Fund
Public Citizen

[54] ESMA, "Sustainable Finance Roadmap 2022-2024," 10 Feb. 2022. https://www.esma.europa.eu/sites/default/files/library/esma30-379-1051_sustainable_finance_roadmap.pdf

[55] CME Group, "Margin: Know What's Needed," Accessed 18 Sept. 2023. https://www.cmegroup.com/education/courses/introduction-to-futures/margin-know-what-is-needed.html; "Bitcoin Futures Contract Specs," *RCM Alternatives*, 14 Nov. 2017. https://www.rcmalternatives.com/2017/11/bitcoin-futures-contract-specs/

[56] Krishna Kumar, Devika , "A month after negative oil prices, U.S. crude contract expiry looms," *Reuters*. 17 May 2020.https://www.reuters.com/article/usa-oil-trading/a-month-after-negative-oil-prices-u-s-crude-contract-expiry-looms-idUSL4N2CX3WH