Google Cloud

February 13, 2023

Submitted via https://comments.cftc.gov

Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street NW
Washington, DC 20581

Re: Reporting and Information Requirements for Derivatives Clearing Organizations
(RIN number 3038–AF12)

Google Cloud welcomes the opportunity to provide comments on the Commodity Futures Trading Commission ("CFTC" or "Commission") proposal to amend Derivatives Clearing Organization (DCO) § 39.18 notification requirements (hereinafter the "NPRM" or "Proposal"). We believe that it is critical that financial regulators, domestically and abroad, continue to modernize and achieve greater convergence in cyber/technology incident reporting. We offer the following comments and feedback to help advance these objectives.

I. Introduction

Effective incident response is critical for the financial markets and services industry and the regulators tasked with oversight of this sector. To this end, achieving greater global convergence regarding related notification and reporting requirements is critical in ensuring that industry actors have clarity and certainty regarding regulatory expectations so that all public and private sector stakeholders can focus on the primary objective of detecting, preventing, mitigating, and responding to cyber incident and technology-related risks that pose a significant likelihood of materially impacting the operations or security of the DCO.

As a provider of cloud services to the financial industry, Google Cloud maintains a rigorous process for identifying, mitigating, and in the event one occurs, responding to and remediating data incidents as part of our overall security and privacy program. We believe strongly in supporting the establishment of effective and consistent global regulatory frameworks governing incident response, including incident reporting requirements.

To this end, we offer below some feedback on the CFTC's proposed amendments to § 39.18. Three high level principles inform our comments, which strike a balance between providing regulators with visibility into potentially significant events, while minimizing the burdens caused by over-reporting on all parties:

1. An important aspect of an effective incident response process is ensuring that true positives/material incidents are promptly flagged to affected customers (and subsequently regulators) and that these are not drowned out by false positives/non-material incidents. This helps service providers, financial institutions ("FIs"), including DCOs, and, ultimately, regulators focus on the incidents that matter and not expend resources on false or *de minimis* matters. To this end, some amount of reasonable investigation is usually required to distinguish true positives/material incidents from false positives/non-material incidents.

2. Consistency regarding notification standards and requirements across domestic and global regulators is critical in enhancing clarity, reducing costly and inefficient fragmentation, and ensuring the objective of identifying and mitigating actual cyber risks. To this end, we encourage the CFTC to incorporate key learnings from the FSB's recent work on incident notification[1] and to conform its practices to the recent updated rules promulgated by the U.S. banking regulators, and urge alignment with regulatory rule-making on incident reporting associated with the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) of 2022.[2] We further encourage the CFTC to establish voluntary fora for information sharing about threats/incidents that can be hosted by the Commission or jointly with other domestic and international regulators.

3. While regulatory clarity is essential for all FIs, including DCOs, it is important that the CFTC also account for the role of service providers with respect to incident notifications and distinctions that may need to be drawn when establishing regulatory expectations relevant to such providers. Our comments below reference examples of regulators recognizing these distinctions and providing helpful clarity to such providers.

II. Feedback on the Proposed Amendments

A. Maintaining a 'Materiality' Threshold

In its Proposal to amend § 39.18, the Commission has suggested eliminating the need for an event to cross a materiality threshold in order to trigger a notification requirement. As an initial matter, given the possible high volume of minor or potential events a DCO and its third-party vendors may face on a regular basis, the elimination of a materiality threshold could not only negatively impact the ability of operators to prioritize incident analysis and remediation efforts, but could also result in

[1] Financial Stability Board (FSB), *Consultative Document: Achieving Greater Convergence in Cyber Incident Reporting* (Oct. 17, 2022), available at https://www.fsb.org/wp-content/uploads/P171022.pdf.
[2] Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), available at https://www.congress.gov/bill/117th-congress/house-bill/2471/text.

significant over-reporting to the Commission, resulting in wasted time and resources across DCOs, their vendors, and Commission staff.

Additionally, the elimination of a materiality threshold would be inconsistent with the FSB's recent recommendations on driving global cyber incident reporting convergence[3] and would move sharply away from final incident notification rules recently promulgated by the U.S. federal banking agencies and proposed by the SEC.[4] Indeed, a move away from regulatory convergence would result in industry actors—DCOs and service providers—spending crucial time and resources navigating regulatory reporting distinctions and operational reporting requirements at the expense of focusing on the primary objective: detecting, preventing, and mitigating incident risks.

With respect to the U.S. banking regulators' recently amended incident notification rules, the agencies specifically referenced and incorporated NIST standards that establish a materiality threshold, and "narrow[ed] the definition of computer-security incident by focusing on actual, rather than potential, harms."[5]

Similarly, in proposing new incident notification requirements for investment advisers, the SEC in 2022 proposed a strong materiality trigger by including only those cybersecurity events that an adviser reasonably believes to be "significant."[6] The Commission's Proposal would move in the opposite direction of its regulatory peers by eliminating a materiality threshold and sweeping in a potentially limitless range of events that are unlikely to pose an actual risk of harm or any cascading impact.

To the extent that the Commission is concerned with the underreporting of events that are subsequently determined to be material, we respectfully suggest that there may be a number of more targeted and efficient ways the CFTC can reduce this underreporting rather than broadening requirements to capture every incident regardless of materiality and actual risk. The FSB has shared regulatory best practices, whereby the regulator uses guidance and other related tools to communicate expectations regarding events that are likely to trigger a materiality threshold. For

---

[3] Financial Stability Board (FSB), *Consultative Document: Achieving Greater Convergence in Cyber Incident Reporting* (Oct. 17, 2022), available at https://www.fsb.org/wp-content/uploads/P171022.pdf.

[4] Federal Reserve System, Office of the Comptroller of the Currency, and Federal Deposit Insurance Company, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers* (Apr. 1, 2022), available at https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211118a1.pdf; Securities and Exchange Commission, *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, Rule Proposal, available at https://www.sec.gov/rules/proposed/2022/33-11028.pdf.

[5] Federal Reserve System, Office of the Comptroller of the Currency, and Federal Deposit Insurance Company, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers* (Apr. 1, 2022), pp. 12, available at https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211118a1.pdf.

[6] Securities and Exchange Commission, *Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies*, Rule Proposal, available at https://www.sec.gov/rules/proposed/2022/33-11028.pdf.

example, the FSB references the Hong Kong Monetary Authority's (HKMA) incident reporting guidelines for offering industry stakeholders a list of examples of incidents that the regulator either would or would not deem to require reporting.[7] Consistent with this best practice, the U.S. banking regulators similarly included in their final rule a list of incidents that would generally be considered "notification incidents."[8] In order to address the evolving risk landscape, the CFTC could adopt these same regulatory tools and update such incident lists based upon industry engagement, emerging best practices, and identification of new threats as they materialize.

The use of guidance or rulemaking, as demonstrated by the U.S. banking regulators, where the regulator provides examples of events that are likely to be material is a more efficient and effective way to ensure proper incident notification reporting. The costs to industry and the regulator will be much lower, confusion and complexity in satisfying fragmented reporting requirements across regulators would be reduced, and industry and CFTC staff will be able to focus their time and resources on identifying and mitigating actual, material risks.

B. Convergence on a "Reasonably Likely" Probability Threshold

The Proposal includes amendments to existing notification requirements by adopting new § 39.18(g)(2), which would strike the term "targeted" before "threats" and change the probability standard from one of "significant likelihood" to include instead notification for events that "could compromise the confidentiality, availability, or integrity of any automated system, or any information, services, or data, including, but not limited to, third-party information, services, or data, relied upon by the DCO in discharging its responsibilities" (emphasis added). Similar to the proposed deletion of a materiality trigger, this proposal would result in overbroad and inefficient reporting, waste critical industry and regulator time and resources, and be inconsistent with domestic and international regulatory best practices.

More specifically, FIs and third-party vendors face a complex threat landscape, which includes frequent, attempted cyber attacks.[9] While such threats and attacks are commonplace, they do not all pose equal risks. Unfortunately, even inconsequential events would be captured by the Proposal's language. Requiring reporting of such events would likely flood the CFTC with notifications and distract attention from material risks.

---

[7] Financial Stability Board (FSB), *Consultative Document: Achieving Greater Convergence in Cyber Incident Reporting* (Oct. 17, 2022), pp. 15 Box 2, available at https://www.fsb.org/wp-content/uploads/P171022.pdf.

[8] Federal Reserve System, Office of the Comptroller of the Currency, and Federal Deposit Insurance Company, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers* (Apr. 1, 2022), pp. 28-29, available at https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211118a1.pdf.

[9] A recent survey found that global organizations reported 925 cyber attacks per week. *See* Check Point Research, *Cyber Attacks Increased 50% Year over Year*, available at https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/.

To this end, the FSB recently amended the definition of cyber incident to clarify that "potential incidents" alone are excluded from the definition. Further, the FSB recommended that even when a regulator has explicitly adopted a materiality trigger, the regulator should in addition attach a "likely to breach" probability standard for reporting of events.

In-line with these recommendations, the U.S. banking regulators recently finalized a notification rule that includes a probabilistic reporting trigger. The final rule release specifically notes that "the agencies are narrowing the scope of covered computer-security incidents by substituting the phrase 'reasonably likely to' in place of 'could.' The agencies agree that the term 'could' encompasses more, and more speculative, incidents than the agencies intended in promulgating the rule."[10]

We accordingly recommend that the CFTC move towards regulatory convergence by adopting the same probabilistic trigger as the banking regulators, which will help ensure certainty and consistency for DCOs seeking to comply with notification requirements.

C. Consideration of Third-Party Vendors

The Proposal includes reference to third-party vendors in stating that the DCO "notify the Commission upon discovery of any security incidents or threats affecting the information, services, or data that the DCO relies upon from the other entity, just as if the incident or threat had occurred at the DCO." The Proposal lacks, however, detailed consideration of how the changes to the materiality thresholds and reporting requirements will impact such vendors and their ability to support DCO compliance with the rules. As noted above, for example, an overbroad notification requirement that lacks a materiality trigger will likely result in certain vendors being required to report volumes of insignificant events to the DCO, which will then be required to sort and report such information to the CFTC.

For this reason, we recommend that the Commission assess the full costs and operational considerations of modifying the existing reporting requirements for both the DCOs and their third-party vendors. For their part, the U.S. federal banking agencies included detailed discussion regarding their notification expectation for vendors, including with respect to timeliness and materiality. We encourage the Commission to reference the U.S. banking regulators' approach as a best practice and one that can advance regulatory convergence for all involved stakeholders. With such clarity, service providers and FIs, including DCOs, will then be in a position via contracting to ensure proper communication between the companies, shared understanding of regulatory expectations, and efficient incident notification processes.

[10] Federal Reserve System, Office of the Comptroller of the Currency, and Federal Deposit Insurance Company, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers* (Apr. 1, 2022), pp. 25, available at https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211118a1.pdf.

III. Conclusion

We appreciate the opportunity to provide our views on the Commission's NPRM regarding DCO notification requirements. We have a shared interest in making sure that incidents are managed properly and any risks resulting from incidents are appropriately mitigated. By pursuing convergence with respect to regulatory requirements consistent with domestic and global best practices, the Commission can increase the effectiveness of notification regulations and help safeguard markets.