CME Group

June 5, 2023

VIA ELECTRONIC SUBMISSION

Vanessa A. Countryman
Secretary
Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090

Re: Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents (File Number S7-06-23) and Regulation Systems Compliance and Integrity (File Number S7–07–23)

Dear Sir or Madam:

CME Group Inc. ("CME Group"),[1] on its own behalf and on behalf of its wholly-owned subsidiary, BrokerTec Americas LLC ("BrokerTec"), appreciates the opportunity to comment on the Securities and Exchange Commission's ("SEC" or "Commission") Proposed Rule regarding Cybersecurity Risk Management Rule for Broker-Dealers, Clearing Agencies, Major Security-Based Swap Participants, the Municipal Securities Rulemaking Board, National Securities Associations, National Securities Exchanges, Security-Based Swap Data Repositories, Security-Based Swap Dealers, and Transfer Agents ("Proposed Rule 10") and the Commission's Proposed Rule regarding Regulation Systems Compliance and Integrity ("Proposed Reg SCI") (collectively the "Proposed Rules").[2]

BrokerTec Americas LLC ("BrokerTec"), a wholly-owned subsidiary of CME Group, is registered as a broker-dealer with the SEC and is also a member of the Financial Industry Regulatory Authority ("FINRA"). BrokerTec's primary offering is a fully electronic trading platform that provides a central limit order book ("CLOB") for the trading of U.S. Treasury securities to the professional trading community of banks, dealers, and proprietary trading firms. This includes purchases and sales of U.S. Treasury securities as well as repurchase agreements involving U.S. Treasury securities. BrokerTec also offers a direct streaming platform for U.S. Treasury securities and a request for quote ("RFQ") platform for repurchase agreements involving U.S. Treasury securities. BrokerTec averages approximately 75,000

[1] CME Group, a corporate holding company, wholly owns Chicago Mercantile Exchange Inc. ("CME"). CME is registered as a derivatives clearing organization ("DCO") ("CME Clearing") with the Commodity Futures Trading Commission ("CFTC"). CME Clearing offers clearing and settlement services for futures and options contracts, including those listed on CME Group's CFTC-registered designated contract markets ("DCMs"), and cleared swap derivatives transactions. These DCMs are CME, Board of Trade of the City of Chicago, Inc. ("CBOT"), New York Mercantile Exchange, Inc. ("NYMEX"), and the Commodity Exchange, Inc. ("COMEX") (collectively, the "CME Group Exchanges" or "Exchanges"). Through the Exchanges, CME Group offers the widest range of global benchmark products across all major asset classes based on interest rates, equity indexes, foreign exchange, energy, agricultural products, and metals.

[2] 88 FR 20212 (April 5, 2023) and 88 FR 23146 (April 14, 2023).

trades per day with an average total notional volume (single-sided) of over $100 billion per day in U.S. Treasury securities on the CLOB.

***

I. EXECUTIVE SUMMARY

The matters addressed by the Proposed Rules are critically important, and CME Group supports the Commission's goals of ensuring that crucial components of the U.S. securities markets are resilient in the face of cybersecurity and other risks.

As a general matter, we support proposals that would strengthen the financial markets' cybersecurity defenses. However, we have concerns with specific elements of Proposed Rule 10. Namely, we believe that the notification and disclosure requirements could have unintended negative consequences. We thus recommend modifying them to make them more practicable for market participants without compromising the Commission's goal of robustly guarding against cybersecurity risks.

With respect to Proposed Reg SCI, we note that certain elements are duplicative of Proposed Rule 10 and other existing regulations. We encourage the Commission to collaborate with and defer to other agencies with statutory authority and deep expertise in systems integrity to avoid imposing duplicative or counterproductive requirements. Relatedly, the Proposed Rules carry significant costs, and we believe that certain of the estimates set forth are unrealistically low. Further, as detailed below, some provisions are practically unworkable and would unduly increase the burdens of compliance without fundamentally enhancing the resiliency of the U.S. securities markets. The Commission thus should revise its proposals to support stronger system resiliency without mandating excessive and duplicative reporting and other requirements.

Ultimately, we recommend that Rule 10 be adopted first, subject to limited modifications discussed below, and that BrokerTec and similarly situated broker-dealers be excluded from the scope of Reg SCI until such time as the Commission can evaluate whether the benefits achieved from Rule 10 are sufficient to achieve the Commission's stated goals.

II. PROPOSED RULE 10

Under Proposed Rule 10, the Commission would amend existing recordkeeping rules to require certain entities ("Market Entities"), including broker-dealers among others, to address cybersecurity risks through: (i) policies and procedures, (ii) immediate notification to the Commission of the occurrence of a significant cybersecurity incident and the reporting of detailed information to the Commission about a significant cybersecurity incident, and (iii) certain public disclosures.

We agree that U.S. securities markets are part of the critical infrastructure of the United States and that their fair, orderly, and efficient operation hinges on the ability of financial institutions to carry out their critical functions. We further agree that it is of paramount importance for Market Entities to take steps to protect their systems from cybersecurity risks. There are, however, certain proposed requirements that we

believe should be modified to retain the benefits of transparency and resiliency, while reducing what would otherwise be significant burdens on Market Entities and the risk of unintended negative consequences.

A. Notification & Reporting Requirements

Proposed Rule 10 would require all Market Entities to give the Commission immediate written electronic notice of a significant cybersecurity incident upon having a reasonable basis to conclude that a significant cybersecurity incident has occurred or is occurring.[3] Additionally, Market Entities would need to report information about the significant cybersecurity incident promptly, but no later than 48 hours, after having a reasonable basis to conclude that the incident has occurred or is occurring by filing Part I of proposed Form SCIR with the Commission.[4] The immediate notice and subsequent reporting requirements are duplicative of existing requirements relating to cyber events such as those required under the Bank Secrecy Act and other SEC requirements, including the requirement on public companies to file Form 8-K.

CME Group is also concerned that the requirements to (i) notify the Commission immediately and (ii) submit a report within 48 hours, provide insufficient timelines. Both requirements will interfere with the ability of Market Entities to address cybersecurity incidents at precisely the wrong time, namely as they are managing the incident response and attempting to limit operational impacts of the incident itself. Devoting time to preparing a substantial report would redirect resources away from effectively responding to the incident. This issue is even more acute where the incident is significant. Moreover, even if a Market Entity has stopped an intrusion, an immediate notification requirement and 48-hour reporting requirement also risk impeding the Market Entity from properly conducting an internal investigation of the potential cyber incident. Further, at a basic level, Market Entities may not know whether an incident is reportable and, even if it were, may simply be unable to provide adequate responses to certain of the questions posed in Part I while they are still in the process of determining the scope and impact of an incident. Additionally, even where relevant information is coming to light during that period, providing a more reasonable period of time would allow Market Entities to prepare a more detailed and, ultimately, more accurate report.

Ultimately, many Market Entities are regulated by numerous agencies on matters relating to cyber security and resiliency. Given existing requirements, we urge the Commission to create a better communication and information sharing policy amongst the relevant agencies and not overburden Market Entities with multiple notification and reporting requirements with varying time deadlines. The Commission should also provide more evidence that these additional requirements would in fact protect and strengthen the financial system's integrity. At this time, it is not clear that requiring immediate notifications and 48-hour reports would do much more than impose undue burdens on market participants and detract from responding to actual intrusions.

Should the Commission determine that a notification or report is necessary, we note that other well-regarded cybersecurity regimes, such as the Cyber Incident Reporting for Critical Infrastructure Act of

[3] See paragraph (c)(1) of proposed Rule 10.
[4] See paragraph (c)(2) of proposed Rule 10.

2002 ("CIRCIA"), provide 72 hours for a covered cyber incident report to be submitted.[5] We believe that this timeline is appropriate and that the Commissions should eliminate the notification requirement and adopt a 72-hour timeline for the Proposed Rule 10 reporting requirement. This would provide the Commission with prompt notification while also allowing Market Entities to appropriately manage the immediate aftermath of a cybersecurity incident.

B. Public Disclosure

Under Proposed Rule 10, Market Entities would also be required to prepare public disclosures on Part II of proposed Form SCIR about their cybersecurity risks and the significant cybersecurity incidents they experienced during the current or previous calendar year.[6] Additionally, Market Entities would be required to "promptly update" the disclosure after the occurrence of a new significant cybersecurity incident or when information about a previously disclosed significant cybersecurity incident materially changes.

These public disclosures present a significant risk of unintentionally assisting the malicious actors against whom Market Entities have crafted their cybersecurity defenses, and we do not believe it is prudent to require Market Entities to provide them. Namely, were a Market Entity to experience a cybersecurity incident, it could be required to disclose the incident while it is ongoing or while the Market Entity is still in the process of repairing and remediating its systems. Moreover, and of even greater concern, Market Entities would be required to state explicitly that the incident is ongoing and/or the Market Entity is still in the process of remediating the incident. This public disclosure would result in significant additional exposure for a Market Entity during such period of time and risks inviting an attempted intrusion by a bad actor by highlighting the Market Entity's state of vulnerability and potentially flagging a point of entry. Further, even where an incident has been fully resolved, publicly disclosing information—even at a summary level—could provide prospective bad actors a roadmap of the vulnerabilities at a given Market Entity, as well as similarly situated Market Entities.

As stated above, we do not believe Market Entities should be required to provide the disclosures on Part II of proposed Form SCIR. Should the Commission determine nonetheless that such disclosures are necessary, we would encourage the Commission to extend the timeframe for updating the disclosures. The requirement to *promptly* update the public disclosure raises concerns similar to those discussed above regarding the immediate notification and reporting requirements. A Market Entity's primary focus in the immediate aftermath of a cybersecurity incident is and should be to ensure that the incident is stopped and to commence an investigation to understand how it happened, in order to ensure that the Market Entity is not exposed to the same vulnerabilities elsewhere or in the future. To layer on a requirement to update disclosures at the same time would divert this focus and the resources that must be devoted to it. Further, from a practical perspective, immediately following the initial discovery of a cybersecurity incident, there may be a dearth of accurate information and facts. Facts that appear to be true initially may turn out to be incorrect as additional information comes to light. For the same reasons, Market Entities should not be rushed into making materiality or significance determinations. Premature disclosure will cause more

[5] CIRCIA requires certain critical infrastructure entities to report on a confidential and protected basis covered cyber incidents to the Cybersecurity and Infrastructure Security Agency ("CISA") within 72 hours.
[6] See paragraph (d) of proposed Rule 10.

harm than good to market participants, because they will be making decisions based on information that may be incomplete or inaccurate and without the full context that additional time can provide.

C. Costs

As noted above, it appears that certain costs are underestimated. To take one example, the Commission estimates that the annual internal costs for Market Entities to fill out and file both an initial and amended Part I of proposed Form SCIR would be $1,077.50. These costs are based on a blended rate of $431 for an assistant general counsel and compliance manager for a total of 2.5 hours. The Commission estimates annual external costs to be $992 per Market Entity, based on using legal counsel at a rate of $496 per hour for a total of two hours.[7] We believe that almost all of the inputs are underestimated, including the number of internal staff involved, the number of hours required, and the billing rate and amount of time required of external counsel. For example, were a significant cybersecurity incident to occur and the submission of Part I of Form SCIR be required, it would likely include involvement and input from multiple legal and compliance resources, in addition to internal stakeholders from operations, technology, information governance and other support functions, contributing to more personnel and more time devoted to the submission of Part I.

III. PROPOSED REG SCI

The Commission is proposing amendments to the existing Regulation Systems Compliance and Integrity (''Reg SCI''). At the highest level, Proposed Reg SCI has two significant impacts: it (1) expands the scope of covered entities and (2) includes substantive amendments to certain provisions of the existing regulation that would impose significant new costs on those covered entities. Pursuant to Proposed Reg SCI, the following entities would become an ''SCI entity'': registered security-based swap data repositories (''SBSDRs''); registered broker-dealers exceeding an asset or transaction activity threshold; and additional clearing agencies previously exempted from registration. The proposed updates would amend provisions of Reg SCI relating to systems classification and lifecycle management; third party/vendor management; cybersecurity; the SCI review; the role of current SCI industry standards; and recordkeeping and related matters. As stated above, and for the reasons described below, we believe that BrokerTec and similarly situated broker-dealers should be excluded from the scope of Reg SCI if subject to Proposed Rule 10.

A. Duplicative

We note that, prior to the publication of Proposed Reg SCI, the Commission had already proposed modifications to Reg SCI and further has simultaneously published Proposed Rule 10. It would be helpful for the Commission to clarify its intentions as there is significant overlap across these proposals. If it is the Commission's intention to pursue each of these rulemakings, we would contend that doing so is inefficient and unnecessary to achieve the resiliency and systems integrity the Commission seeks. Further, as discussed below, Proposed Reg SCI alone presents redundancies for Market Entities[8] that are

[7] Proposed Rule 10 at 20307.

[8] We recognize there is some divergence between entities in scope for Proposed Rule 10 and Proposed Reg SCI. However, for sake of simplicity, we use the term Market Entities throughout.

subject to FINRA rules or comply with similar regulatory regimes, such as the CFTC's system safeguards requirements and Reg ATS's capacity, integrity, and security of automated systems requirements.

Specifically, certain of Proposed Reg SCI's recordkeeping obligations are duplicative of regulations to which SCI entities are already subject. In addition to the duplicative policies and procedures requirements, Proposed Reg SCI creates the risk of subjecting Market Entities to multiple, repetitive reporting requirements to different divisions of the Commission, all while trying to do the critical work of protecting their organizations from a cybersecurity intrusion. In other words, Market Entities would be subject to substantial additional cost without an attendant benefit.

Additionally, Proposed Reg SCI's expansion of entities subject to Reg SCI's annual review requirements would render certain Reg SCI requirements redundant of already applicable FINRA requirements for the newly covered entities. For example, Rule 1003(b) of Reg SCI requires SCI entities to conduct annual reviews of the SCI entity's compliance with Reg SCI, and to submit the report of those reviews to the Commission.[9] However, FINRA Rule 3130 requires all FINRA members (including those who would now be subject to Reg SCI) to certify annually that they have established processes, carried out necessary reviews, and generated compliance reports designed to ensure the member's compliance with "applicable FINRA rules, MSRB rules and federal securities laws and regulations."[10] Notably, "federal securities laws and regulations" would include Reg ATS and cybersecurity rules adopted by the Commission (such as Proposed Rule 10).

B. Additional Considerations

Rule 1002 of Reg SCI requires SCI entities to notify the Commission immediately upon "any responsible SCI personnel having a reasonable basis to conclude that an SCI event has occurred."[11] SCI entities are also required to submit a written notification to the Commission within 24 hours, and to provide periodic updates to the Commission "[u]ntil such time as the SCI event is resolved and the SCI entity's investigation of the SCI event is closed."[12] We believe that expanding both the scope of SCI entities subject to these reporting requirements and the types of incidents that qualify as SCI events presents real risks by requiring the reporting of immaterial events, which will divert resources of the Commission and market participants. Critically, when an incident occurs it will, in many cases, take time to determine whether it qualifies as an SCI event. Requiring immediate notice will invariably result in the reporting of events that do not actually qualify. Further, the individuals responsible for making a determination as to whether an event is reportable will likely overlap with those responsible for returning the system to full functionality. We assume that the Commission would agree that the latter objective ought to be the primary focus when a disruption occurs. Should the Commission proceed with the proposed expansion of Reg SCI, we encourage the Commission to modify the existing timelines included in Rule 1002.

[9] Reg SCI, Rule 1003(b).

[10] FINRA Rule 3130.

[11] Reg SCI, Rule 1002(b)(1).

[12] Reg SCI, Rule 1002(b)(3).

The foregoing issues are further compounded by the expansion of the definition of a "systems intrusion." Most importantly, the proposed expansion would include a "significant attempted unauthorized entry." The requirement to provide information about unsuccessful attempts would be of little value to the Commission and risks creating an influx of unnecessary data that will drown out the information that the Commission would actually need to evaluate the integrity and safety of the U.S. securities markets.

Lastly, we have concerns about the indirect impact of Proposed Reg SCI on the third-party provider ecosystem, specifically regarding cloud service providers ("CSPs"). Rule 1001(a)(2)(v) requires that SCI entities have policies and procedures setting forth business continuity and disaster recovery ("BCDR") plans that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse and that are reasonably designed to achieve next business day resumption of trading and two-hour resumption of critical SCI systems following a wide-scale disruption. With Proposed Reg SCI, the Commission would also require that such plans be reasonably designed to address the unavailability of any third-party provider that provides functionality, support, or service to the SCI entity, without which there would be a material impact on any of its critical SCI systems.[13] The Commission justifies this additional requirement by observing that "SCI entities have become increasingly dependent on third parties—such as cloud service providers—to operate their businesses and provide their services."[14] The proposed BCDR requirements related to third-party providers would, according to the Commission, ensure that SCI entities are prepared for extended outages due to a third-party provider going into bankruptcy or breaching a contract and unilaterally ceasing to provide service. As a general matter, we support requirements that SCI entities maintain BCDR plans, including with respect to third-party providers whose unavailability would materially impact critical SCI systems, as determined by SCI entities. However, we urge the Commission to be cautious with respect to the specific requirements it places on Market Entities and their use of CSPs that provide functionality, support, or service to critical SCI systems. In particular, while the Commission has not gone so far as to do so here, we would stress that mandating prescriptive requirements, such as a multi-cloud arrangement or "on-premises" backups, would introduce additional costs and complexity and, accordingly, additional operational and cybersecurity risks.

Ultimately, we would recommend that the Commission adopt a more flexible principles-based approach to modifying Reg SCI, if any such modifications are necessary. Market Entities should be able to satisfy the Commission's overarching goals of systems integrity and resilience by demonstrating compliance with other proposed and existing frameworks such as Proposed Rule 10, existing FINRA requirements or other comparable regimes already established by other domestic regulators.

C. Costs

We urge as a general matter that the Commission consider the costs carefully, as they are substantial, and whether its proposed approach is appropriately tailored to the market participants to which it will apply. We note that each aspect of Proposed Reg SCI would introduce monitoring, reporting, and other requirements, which will result in substantial monetary costs and demands on personnel resources. Furthermore, certain of the estimated compliance costs set forth in Proposed Reg SCI are not reasonable.

[13] Proposed Reg SCI at 23246.
[14] Proposed Reg SCI at 23246.

For example, we believe that the immediate notification requirement will consume resources without an attendant benefit and result in over-reporting. In particular, we believe that the estimates of the number of notifications per year and the amount of time that Market Entities would need to devote to such notifications fall short of the likely reality. At bottom, we believe the true substantial costs are not commensurate with the limited benefits, especially in light of the extent of duplication and the unduly compressed timelines for reporting.

***

IV. CONCLUSION

CME Group has long recognized that resilient systems and cybersecurity defenses are fundamental to financial markets. CME Group thus supports the Commission's objective to enhance the requirements around systems integrity for key market participants and bolster protections related to cybersecurity risks. However, CME Group also recognizes that duplicative and overly costly standards can have unintended and disruptive consequences. Additionally, as detailed above, CME Group has specific concerns around the notice and disclosure requirements of the Proposed Rules, among other considerations. In light of these concerns, CME Group recommends that the Commission implement Proposed Rule 10 first, as modified per our comments above, before moving forward with any expansion of Reg SCI.

CME Group appreciates the opportunity to submit these comments to the SEC and looks forward to working with the SEC to strengthen the resilience of the U.S. securities markets. If you have any comments or questions, please feel free to contact me at **(312) 930-2324** or via email at **Jonathan.Marcus@cmegroup.com**.

Sincerely,

Jonathan Marcus

Jonathan Marcus
Senior Managing Director and General Counsel
CME Group Inc.
20 South Wacker Drive
Chicago, IL 60606