Tradeweb

1177 Avenue of the Americas
New York, NY 10036

phone: 646.430.6000
fax: 646.430.6250
email: help@tradeweb.com
www.tradeweb.com

February 22, 2016

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

Re: ***System Safeguards Testing Requirements – 80 Fed. Reg. 80140 (December 23, 2015) (RIN 3038–AE30)***

Dear Mr. Kirkpatrick:

Tradeweb Markets LLC ("***Tradeweb***") welcomes the opportunity to comment on the proposed rule of the Commodity Futures Trading Commission ("***Commission***" or "***CFTC***") regarding system safeguards for designated contract markets, swap execution facilities, and swap data repositories (the "***Systems Safeguards Proposal***").

Since 1998, Tradeweb has offered electronic trading systems for fixed income investors in the United States and abroad, and has played an important role in providing greater transparency in and improving the efficiency of the trading of fixed income securities and derivatives. Indeed, Tradeweb has been at the forefront of creating electronic trading solutions which support price transparency and reduce systemic risk, which are the hallmarks of Title VII of The Dodd-Frank Wall Street Reform and Consumer Protection Act (the "***Dodd-Frank Act***")[1]; accordingly, Tradeweb is supportive of the Dodd-Frank Act and its stated policy objectives relating to Title VII. Tradeweb also has been an active participant in the ongoing public debate around swap execution facilities ("***SEFs***"), how best to bring greater transparency and accountability to the derivatives market, and the implementation of Title VII of the Dodd-Frank Act. Tradeweb has two SEFs that were granted permanent registration on January 22, 2016 – TW SEF LLC and DW SEF LLC.

As a leader in electronic trading, Tradeweb adheres to generally accepted standards and industry best practices, including for its two SEFs, in its programs of risk analysis and oversight with respect to its operations and automated systems for the areas outlined in the Systems Safeguards Proposal: enterprise risk management and governance, information security, business continuity-disaster recovery planning and resources, capacity and performance planning, systems operations, systems development and quality assurance, and physical security and environmental controls. For this reason and the reasons set out more fully below, Tradeweb has a significant interest in the Systems Safeguards Proposal regarding proposed amendments to the CFTC's system safeguards rules.

Tradeweb strongly supports the principles-based testing standards in the Systems Safeguards Proposal, particularly because the SEF regulatory regime is still in its early stages. While we note some areas

[1] Pub. L. 111-203, 124 Stat. 1376 (2010).

where additional guidance would assist SEFs, Tradeweb believes that flexibility in demonstrating compliance is critical as the CFTC begins to regulate SEFs in full, and as market participants expand their usage of SEFs. Further, principles-based standards permit entities to address the CFTC's cybersecurity concerns, while also adapting to technological changes and the evolving nature of cyber threats. It also allows SEFs to address these issues in the context of the different models and technology they offer. Therefore, as discussed below, Tradeweb believes that the CFTC should take a measured and analytical approach to the full implementation of a final systems safeguards rule, which includes phased compliance and further study with the participation of the SEFs and market participants. In Section I., we discuss our general observations related to the Systems Safeguards Proposal's discussion of so-called "Covered SEFs" and in Section II., we provide specific recommendations related to amendments to specific aspects of the Systems Safeguards Proposal.

I. The Commission Should Engage Directly with SEFs in an Appropriate Forum Regarding the Concept of Covered SEFs

As a leading technology firm, Tradeweb supports CFTC rulemaking designed to ensure the effectiveness of cybersecurity testing and the adequacy of programs of system safeguards risk analysis and oversight. Nevertheless, the CFTC only last month began to issue orders permanently approving SEF registrations, and, as the Commission points out, the SEF market is still in an early stage of development.[2] The tentative proposal to subject certain SEFs to minimum testing frequency requirements and independent contractor testing as Covered SEFs should therefore be carefully considered by the Commission, in dialogue with the SEFs to whom these rules would potentially apply; particularly because the rules could disproportionately impact certain SEFs. To that end, the Commission should consider whether, given the number of SEFs and the horizontal nature of swaps trading, such tentative proposed rulemaking should cover all SEFs rather than just systemically important SEFs. Therefore, we urge the Commission to set up a roundtable or working group for SEFs – or some other appropriate forum – to solicit discussion on the nature and scope of any future SEF-specific systems safeguards proposed rulemaking, including Covered SEFs.

We also welcome the opportunity to provide specific comments on certain questions set forth in the Systems Safeguards Proposal as follows:

- With respect to Question 1, we believe that the determination of whether minimum testing frequencies should apply to SEFs requires further input which may, if appropriate, result in proposed rulemaking subject to further industry comment.

- With respect to Question 2, given that the SEF market is in an early stage of development, we believe that the definition of "Covered SEF" requires further study and discussion with the industry. As mentioned above, such study and discussion should touch on whether any SEF-specific systems safeguards proposed rulemaking should apply to all SEFs rather than just Covered SEFs. To the extent the Covered SEF concept is incorporated in such systems safeguards proposed rulemaking, any analysis on how to define a "Covered SEF" also should take into account: (i) the extent to which a SEF has widespread electronic distribution, (ii) the types of users who are accessing a SEF and how users access a specific SEF, (iii) how many users

[2] *See* 80 Fed. Reg. at 80161.

a SEF has, and (iv) overall connectivity with other industry market infrastructures (*e.g.*, clearinghouses, futures commission merchants, aggregation services, market data, compression, and other post-trade utilities, and other external market connectivity). These factors are important when considering cyber threats to electronic trading systems.

- With respect to Question 7, we believe that any minimum testing frequency and independent contractor testing requirements should apply to all SEFs, not just Covered SEFs. Given the early stage of development of the SEF market, the commercial viability of SEFs – even systemically important SEFs – will be sensitive to additional regulatory requirements. Furthermore, from a policy perspective, the Commission must ensure that all SEFs are appropriately and adequately addressing cybersecurity and system safeguards. The Commission should follow its own precedent with regard to batch registration of SEFs and make sure that: (i) system safeguard rules do not put certain SEFs at a competitive disadvantage vis-à-vis other SEFs, and (ii) the entire SEF market is robust from a cybersecurity perspective. Tradeweb therefore believes that any minimum testing frequency and independent contractor testing requirements should apply to all SEFs. While the Commission has set forth rules for "covered designated contract markets," such a market construct, which is largely a vertical model, differs greatly from the SEF market construct, which is horizontal (i.e. many SEFs offering the same instruments and multiple access points).

- With respect to Question 9, we believe that the determination of the benefits and costs of applying the minimum testing frequency and independent contractor testing requirements to Covered SEFs requires further industry comment and discussion. The calculation of cost is complex and requires consideration of various factors, including but not limited to: (i) the hiring of independent contractors who can perform such tests, (ii) whether any new rule will necessitate the addition of dedicated staff, and (iii) additional employee-hours spent in overseeing the testing. In order to allow the Commission to make an accurate cost-benefit analysis of this rulemaking, we recommend that the Commission provide a forum or other opportunity for industry participants to discuss with the Commission the potential costs related to the implementation of the Systems Safeguard Proposal.

In addition to the above, the Commission should also consider the cross-border scope and impact of any systems safeguards rulemaking. Tradeweb currently operates regulated platforms outside of the United States, including a multilateral trading facility, offering similar functionality as offered to U.S.-based clients through Tradeweb's U.S.-regulated entities. We therefore believe that these rules will also have implications for both inbound and outbound U.S. swap transactions. We recommend that the Commission should also solicit comment on the Systems Safeguards Proposal from international regulators independently or at a working group or roundtable.

II. Phased Implementation and Enhancements to the Systems Safeguards Proposal

We believe that there are a number of ways in which the CFTC may enhance further enhance the Systems Safeguards Proposal, to enhance SEF cyber resilience in accordance with generally accepted standards and industry best practices:

First, the Commission should specify an adequate implementation period for the finalized system safeguard rules. We recommend an implementation period (e.g., 9-12 months) that is sufficient to prepare and implement any additional policies and procedures required under the Systems Safeguards Proposal.[3]

Second, there are a number of other areas where the Systems Safeguards Proposal can be clarified:

- The proposed rules can currently be read to suggest that a successful cyberattack on a SEF would result in an enforcement action against the SEF for inadequate testing under the system safeguards rules.[4] This would be unnecessarily punitive to SEFs that may nevertheless have attempted to comply with the system safeguards rules in good faith. We believe that in order to set clear expectations for SEF cybersecurity, the Commission should:
    - designate certain standards that would function as safe harbors under all the testing and assessment requirements set forth in proposed CFTC Regulation 37.1401(h).[5] For example, conducting an evaluation of the threats identified in the Open Web Application Security Project Top 10 critical web application security risks list[6] could be regarded as sufficient to fulfill the vulnerability testing requirement specified in proposed CFTC Regulation 37.1401(h); and
    - provide clear guidance on what constitutes "timely" remediation under proposed CFTC Regulation 37.1401(m). Given the complexity of certain types of remediation, we recommend a safe harbor from the date that the deficiency or vulnerability necessitating remediation is discovered (e.g., 9-12 months depending on the issue and the extent of the remediation required). Without clear guidance in this respect, a SEF experiencing a cyberattack that implicates a to-be-completed remediation would be faced with a concomitant enforcement action. We believe this result is also unnecessarily punitive to a SEF and contrary to the spirit of the Systems Safeguards Proposal.
- External penetration testing should be clearly defined to mean penetration testing conducted over the internet.
- The Commission should provide further guidance on how controls testing differs from vulnerability testing. Specifically, Tradeweb requests clarification from the Commission on whether: (i) industry standards such as SSAE16 Type 2 or SOC1 annual audits can be expanded and utilized for controls testing purposes and (ii) annual independent black and gray box penetration tests can be used to fulfill the vulnerability testing and controls testing requirements in proposed CFTC Regulation 37.1401(h).

[3] *See also* Appendix 4 —Statement of Commissioner J. Christopher Giancarlo of 80 Fed. Reg. at 80190-91 (stating that "I also believe that the CFTC should provide a sufficient implementation period for any final rules so that market operators, especially smaller DCMs and SEFs, have adequate time to meet the new requirements.")

[4] *Id.* at 80191 (stating that "Market participants who abide by the rule should not be afraid of a 'double whammy' of a destructive cyber-attack followed shortly thereafter by a CFTC enforcement action.")

[5] We note that Commissioner Giancarlo also suggested the implementation of certain safe harbors for compliance with the proposed rules. *Id.*

[6] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

- The security incident response plan evaluation in proposed CFTC Regulation 37.1401(h)(5) is duplicative of the other testing requirements in other areas of proposed CFTC Regulation 37.1401(h). While Tradeweb agrees that having a security incident response plan is essential to the functioning of a SEF, a security incident response plan need only be reviewed annually and approved by an individual at the SEF in charge of information security. Requiring repeated testing of such plans is burdensome, unduly costly, and arguably overlaps with remediations undertaken in connection with testing specified in other areas of proposed CFTC Regulation 37.1401(h).

- The enterprise technology risk assessment in proposed CFTC Regulation 37.1401(h)(6) is also duplicative of the other testing requirements in other areas of proposed CFTC Regulation 37.1401(h). While Tradeweb agrees that being cognizant of enterprise technology risks is essential to the functioning of a SEF, we believe that such a risk assessment need only be reviewed annually and approved by an individual at the SEF in charge of information security. Requiring repeated assessments is burdensome, unduly costly, and overlaps significantly with testing and related remediations undertaken pursuant to other areas of proposed CFTC Regulation 37.1401(h).

III. Conclusion

Tradeweb understands that the Commission has the difficult task of balancing its own underlying regulatory concerns with concerns about the imposition of additional cost on industry participants. We believe that certain practical considerations related to SEFs that we have highlighted above will allow the Commission to issue a final rule with phased compliance that ensures robust cybersecurity safeguards, while avoiding the possibility of disruption to the existing SEF market. Tradeweb would also be available to participate in the roundtables or working groups discussed above.

* * * * * *

If you have any questions concerning our comments, please feel free to contact the undersigned.
Tradeweb welcomes the opportunity to discuss these issues further with the Commission and its staff.

Respectfully submitted,

Douglas Friedman
General Counsel

cc: Honorable Timothy Massad, Chairman
Honorable Sharon Bowen, Commissioner
Honorable J. Christopher Giancarlo, Commissioner