WMBA
AMERICAS
WHOLESALE MARKETS BROKERS' ASSOCIATION

February 22, 2016

Mr. Christopher Kirkpatrick, Secretary
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, N.W.
Washington, D.C. 20581

Re: System Safeguards Testing Requirements – Proposed Rulemaking [RIN No. 3038-AE30]

Dear Mr. Kirkpatrick:

The Wholesale Markets Brokers' Association, Americas ("WMBAA" or "Association")[1] appreciates the opportunity to provide comments to the Commodity Futures Trading Commission ("CFTC" or "Commission") regarding the Commission's proposed System Safeguards Testing Requirements rulemaking ("Proposed Rules").[2] The WMBAA recognizes the importance of cybersecurity measures, and the member firms take seriously their respective responsibilities with respect to maintaining a robust cybersecurity program for their swap execution facilities ("SEFs").

As a preliminary matter, the WMBAA extends its appreciation to the Commission for granting permanent registration to each of the member firms' SEFs earlier this year. This milestone represents a significant step toward firmly establishing the regulatory regime for mandatory trade execution as envisioned by the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") and providing market participants with further much-needed regulatory certainty. Against the backdrop of permanent SEF registration, the WMBAA looks forward to continuing to work with the Commission and its staff on all matters pertaining to SEFs, including not only with respect to the Proposed Rules, but also on any future CFTC rulemakings, amendments, guidance, or interpretations related to trade execution and SEFs.

In terms of the Proposed Rules, the WMBAA appreciates the Commission's efforts to clarify existing provisions related to system safeguards risk analysis and oversight and cybersecurity testing for SEFs. While the WMBAA appreciates the Commission's efforts to clarify the existing system safeguards rules for SEFs, the WMBAA encourages the CFTC to harmonize its cybersecurity regulations with international standards and the regulations of other domestic regulatory authorities, including the Securities and Exchange Commission, the Financial Industry Regulatory Authority,

---

[1] The WMBAA is an independent industry body representing the largest inter-dealer brokers. The founding members of the group—BGC Partners, GFI Group, Tradition, and Tullett Prebon—operate globally, including in the North American wholesale markets, in a broad range of financial products, and have received permanent registration as swap execution facilities. The WMBAA membership collectively employs approximately 4,000 people in the United States; not only in New York City, but in Stamford and Norwalk, Connecticut; Chicago, Illinois; Jersey City and Piscataway, New Jersey; Raleigh, North Carolina; Juno Beach, Florida; Burlington, Massachusetts; and Dallas, Houston, and Sugar Land, Texas. For more information, please see www.wmbaa.com.

[2] System Safeguards Testing Requirements, 80 Fed. Reg. 80,140 (Dec. 23, 2015) ("Proposed Rules").

and the National Futures Association, to ensure that the various regulatory regimes do not conflict or cause unnecessarily duplicative requirements for regulated entities. Further, the WMBAA emphasizes the need for cybersecurity rules to be principles-based and provide SEFs with maximum flexibility to construct cybersecurity programs that are based on an individual entity's respective risk assessments. Currently, the WMBAA member firms conduct a multitude of cybersecurity tests on their respective systems, processes, and controls, using both internal and third-party resources.

The WMBAA focuses the remainder of its comments on the following aspects of the Proposed Rules: (1) the contemplated scope of testing and assessment; (2) the systems that should be included within the scope of testing; (3) compliance standards in the testing context; (4) the "covered SEF" concept; and (5) SEF system safeguards-related books and records obligations.

Scope of Testing and Assessment

While the WMBAA appreciates the Commission's consideration of the testing required for SEFs, the WMBAA is concerned that the scope of testing and assessment under the Proposed Rules would set an impracticable standard for SEFs to achieve. Under section 37.1401(k) of the Proposed Rules, the Commission proposes to define the scope of testing and assessment as "broad enough to include all testing of automated systems and controls necessary to identify any vulnerability which, if triggered could enable an intruder or unauthorized user or insider to" cause various interferences.[3] It is not possible, however, for an entity to guarantee that any vulnerability or flaw in a system will be uncovered by testing and to test all automated systems related to a SEF.

The WMBAA questions whether penetration testing firms would be willing to certify that their testing procedures meet such an unbounded standard. Following the release of the Proposed Rules, the WMBAA discussed with a prominent penetration testing firm the proposed scope of testing and inquired as to whether such scope could realistically be achieved. In response, this particular penetration testing firm stated that it would not be able to provide absolute guarantees with respect to the identification of all vulnerabilities or flaws and explained that, given that the dynamic nature of testing is a point-in-time assessment, certain flaws are timing-based or not reproducible regularly.

Based on the WMBAA member firms' experiences, two penetration testing companies might find different vulnerabilities depending on the creation of the test. In addition, there are myriad avenues for potentially penetrating a SEF's system, but it is impracticable to test them all. Accordingly, the inability of entities to test for every potential vulnerability underscores the importance of properly determining the scope of testing.

[3] *See* Proposed Rules, at 80,183 (emphasis added).

Scope of Systems to Be Tested

In terms of the scope of systems that should be tested with respect to SEFs,[4] due to the architecture of systems in which SEFs operate, the WMBAA does not believe that the Commission's cybersecurity rules should focus on testing from a SEF system's perimeter, but rather should require testing and oversight of the major components surrounding a SEF system.[5] In complying with such a requirement, SEFs should be permitted to identify the systems supporting the SEF's functionality that should be subject to cybersecurity testing.

Based on the WMBAA members' experiences, a SEF system is typically a subset of a larger financial services company's operating systems, surrounded by other data centers and bolt onto the systems of the broader entity, rather than a freestanding network. Even if a SEF has its own system, it typically does not have its own dedicated security defense systems and separate cybersecurity procedures and testing, but rather is part of a larger integrated system that provides such defenses and cybersecurity procedures and testing for the entity as a whole, including those mechanisms unique to the SEF. As a result, the WMBAA is unaware of an industry cybersecurity practice that specifically focuses on testing an internal system like that of a SEF system and believes that the value of such testing would be inconsistent with prevailing industry practice and have extremely limited value.

Rather than focusing on the testing of a SEF system's perimeter, the WMBAA recommends that the Commission's cybersecurity regulations establish broad principles, permitting SEFs to define the scope of testing by considering the systems surrounding the SEF and determining which of these systems are primary and secondary in terms of their interactions with the SEF.

Compliance Standards

In addition to the issues regarding the proposed scope of testing, the WMBAA is concerned that, under the Proposed Rules, notwithstanding the presence of robust cybersecurity measures, an entity compromised by a cyber-attack would be found to be in violation of the CFTC's testing and remediation rules. The regulations should encourage close cooperation between the SEFs and the Commission and not play "gotcha" when an intrusion is discovered, as no cybersecurity program can guarantee absolute protection.

The WMBAA member firms take seriously their respective responsibilities with respect to cybersecurity and currently oversee robust cybersecurity programs covering the systems that include SEFs. Despite best efforts in accordance with industry standards and practices, SEFs cannot absolutely guarantee that their systems are impervious to any intrusion. In this regard, the WMBAA agrees with Commissioner J. Christopher Giancarlo that "[m]arket participants who abide by the rule should not be afraid of a 'double whammy' of a destructive cyber-attack followed shortly

[4] *See* Proposed Rules § 37.1401(k) (stating "all testing of automated systems").

[5] Such systems include those described in Exhibit V to Form SEF.

thereafter by a CFTC enforcement action," and "[b]eing hacked, by itself, cannot be considered a rule violation subject to enforcement."[6]

To address these concerns, the WMBAA further agrees with Commissioner Giancarlo that the Commission should indicate how it will measure SEFs' compliance against industry standards and designate broad principles and safe harbors for compliance with the rules.[7]

"Covered SEF" Concept

The Commission includes in the Proposed Rules an advance notice of proposed rulemaking regarding minimum testing frequency and independent contractor testing requirements for "covered SEFs," which it is considering defining as "those SEFs for which the annual total notional value of all swaps traded on or pursuant to the rules of the SEF is ten percent (10%) or more of the annual total notional value of all swaps traded on or pursuant to the rules of all SEFs regulated by the Commission."[8]

At this time, the WMBAA respectfully recommends that the Commission decline to propose a "covered SEF" concept that subjects certain SEFs to new minimum testing frequency and independent contractor testing requirements for the following reasons. First, since SEFs function exclusively as trade execution platforms that foster liquidity for swap execution, their operations—irrespective of the total number of swaps traded or notional value of those swaps—do not implicate the same systemic concerns attendant to the failure of or outside penetration of a designated contract market ("DCM") or derivatives clearing organization ("DCO"). Whereas all DCMs, including the larger DCMs, own their contracts, the trading of which is only allowed on their respective exchanges, SEFs do not have any ownership or proprietary control over the products bought and sold on their platforms, and SEFs, unlike DCOs, do not hold customer funds or guarantee performance by counterparties. SEF products trade simultaneously across multiple liquid SEFs as market participants trade on multiple SEFs to seek best execution. If a particular SEF failed or was unable to continue operating in a particular swap market, market participants could readily move their trading to another SEF without difficulty. As a result, developing a "covered SEF" concept out of concern for an individual SEF's purported systemic importance is unfounded.

Further, under the Commission's potential definition of "covered SEF," a SEF may be "covered" one year but not the next, depending on the trading volume on such SEF. Such a mutable status would be problematic for SEFs in terms of regulatory certainty and may require a "covered SEF" to invest significant resources one year to satisfy requirements that may not be applicable the following year. While it is arguably true that the applicability of regulatory requirements in general can change depending on a variety of factors, the regulatory regime surrounding SEFs is relatively new and SEF rules may be further fine-tuned by the Commission. The unsettled nature of the SEF regulatory environment is yet another factor that weighs against the adoption of a "covered SEF" concept.

---

[6] Commissioner Giancarlo Statement Regarding Proposed Rule on System Safeguards Testing Requirements (Dec. 16, 2015), *available at* http://www.cftc.gov/PressRoom/SpeechesTestimony/giancarlostatement121615a.

[7] *See id.*

[8] *See* Proposed Rules, at 80,161.

The WMBAA submits that considerations related to cybersecurity testing frequencies and the use of independent contractors should be left to the discretion of the individual entity based on its risk assessments. The costs associated with the use of independent contractors for cybersecurity testing are high, as third-party resource costs must be considered in addition to employee resource costs. Accordingly, in all instances, SEFs should be permitted to appropriately utilize internal employee resources to mitigate testing costs.

In view of the above, the WMBAA believes that the costs associated with complying with covered SEF requirements, including any additional reporting obligations and uncertainty related to which SEFs are covered, would exceed any benefits to be derived.

System Safeguards-Related Books and Records Obligations

Under the Proposed Rules, each SEF would be required to provide the Commission upon request with "(1) current copies of the BC–DR plans and other emergency procedures; (2) all assessments of the entity's operational risks or system safeguard-related controls; (3) all reports concerning system safeguards testing and assessment . . . whether performed by independent contractors or employees of the . . . SEF . . . ; and (4) all other books and records requested by Commission staff in connection with Commission oversight of system safeguards . . . ."[9]

The WMBAA appreciates that SEFs have statutory and regulatory obligations to produce information pertaining to the business of the facility as the Commission determines to be necessary or appropriate to perform the duties of the Commission under the Commodity Exchange Act.[10] Given the sensitivity of information contained in cybersecurity testing reports, however, the WMBAA respectfully submits that SEFs have a responsibility to engage in sound risk management practices by safeguarding testing results from widespread dissemination. The potential for accidental release or misuse of highly confidential information regarding specific system and process vulnerabilities is magnified when detailed results of penetration tests and vulnerability analyses are made available to parties beyond an entity's management. Such reports contain information that would be detrimental to an entity's core security and could provide a "roadmap" for cyber-attacks in the wrong hands.

Accordingly, as an initial matter upon a Commission request for reports concerning system safeguards testing and assessment, the WMBAA recommends that SEFs be required to provide the Commission with a limited data set of cybersecurity testing results, and then permit CFTC staff to view the original materials in a non-electronic and non-reproducible format.[11] The limited data set could include key performance indicators and executive summaries and could be made available to the Commission in a form and manner determined by the Commission. Subsequently, if the Commission determines further detailed information is necessary, SEFs should be permitted to

[9] Proposed Rules, at 80,162.

[10] *See* CEA § 5h (Core Principle 10).

[11] Based on the WMBAA member firms' experience with the Securities and Exchange Commission, for example, it has not accepted certain electronic documents that it considers to be sensitive, but rather has required onsite paper-based reviews of such information.

provide the Commission with access to original data in a secure, controlled manner, such as through hardcopy documents made available at a SEF office location.

* * * * *

We welcome the opportunity to discuss these comments with you at your convenience. Please feel free to contact the undersigned with any questions you may have on our comments.

Sincerely,

Michael Sulfaro
Chief Compliance Officer
BGC Derivative Markets, L.P.

William Shields
Chief Compliance Officer
GFI Swaps Exchange LLC

Gavin White
Head of Information Security
Tradition

Graham Fair
Global Head of Service Management, IT
Tullett Prebon plc