



February 22, 2016

Via Electronic Submission

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

Re: Comment Letter on Proposed Rulemaking Relating to
System Safeguards Testing Requirements
RIN 3038-AE30, 80 FR 80139 (December 23, 2015)

Dear Mr. Kirkpatrick:

CBOE Futures Exchange, LLC (“CFE”) appreciates the opportunity to provide its comments to the Commodity Futures Trading Commission (“Commission”) regarding the CFTC’s proposal in the above-referenced release (“Release”). The Release proposes to amend the CFTC’s system safeguards rules for designated contract markets (“DCMs”), swap execution facilities (“SEFs”), and swap data repositories (“SDRs”) by augmenting and clarifying existing provisions relating to systems safeguards risk analysis and oversight and cybersecurity testing and by adding new provisions concerning certain aspects of cybersecurity testing.

CFE agrees with the Commission that it is important for DCMs, SEFs, and SDRs to have robust cybersecurity and system safeguards programs. At the same time, CFE believes that any standards that the Commission establishes in this area should be principles-based and not prescriptive. Commission Chairman Timothy Massad observed in his statement regarding the proposal that “[t]he proposal sets forth principles-based testing standards which are deeply rooted in industry best practices.” CFE agrees with this approach and believes that it is important that any Commission enforcement of these standards take the same approach. Establishing or requiring rigid or one-size-fits-all standards does not allow for DCMs, SEFs, and SDRs to appropriately tailor their cybersecurity and system safeguards programs to their own unique systems and infrastructures and does not allow DCM, SEF, and SDR practices and standards to evolve as technology, markets, and best practices evolve. As Commissioner Sharon Bowen observed in her statement regarding the proposal: “[W]e must be careful not to mandate a one-size-fits-all standard because firms are different. . . We need to encourage best practices, while not hampering firms’ ability to customize their risk management plan to address their cybersecurity threats.” In that regard, a DCM, SEF, or SDR should be considered to be in compliance with the proposed standards provided that the entity has undertaken good faith efforts to comply with the standards. These standards should not be enforced in a strict liability manner such that any successful cyber-attack means a violation of the standards must have occurred. Instead, as Commissioner J. Christopher Giancarlo observed in his statement regarding the proposal: “Being hacked, by itself, cannot be considered a rule violation subject to enforcement.”

In order for the standards to be effective, they need to be flexible and allow DCMs, SEFs, and SDRs to implement them in a manner that is appropriate based on their own circumstances and reasonable judgment.

CFE also agrees with Commissioner Giancarlo, as set forth in his statement regarding the proposal, that “the CFTC should provide a sufficient implementation period for any final rules so that market operators . . . have adequate time to meet the new requirements”. DCMs, SEFs, and SDRs need sufficient time to review the final regulations; to compare and apply them to their current cybersecurity testing practices and their current risk analysis and oversight programs in the areas of 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; and to implement any required changes to those practices and programs. Undertaking this process takes time. Not providing sufficient time for review and implementation and rushing this process can increase the very risks that the proposal is intended to safeguard against. CFE notes that when the Securities and Exchange Commission (“SEC”) adopted its comparable regulation (SEC Regulation Systems Compliance and Integrity (“SCI”)), Regulation SCI became effective sixty days after publication in the Federal Register and the SEC adopted a compliance date for Regulation SCI of nine months after its effective date.¹ CFE believes that the Commission should take the same approach with the Commission proposal in the Release and provide for any final regulations to become effective sixty days after publication in the Federal Register and for a compliance date of nine months after the effective date.

CFE is available to provide any further input desired by the Commission regarding the proposal and to work cooperatively with the Commission to address the issues covered by the Release. Please contact me at (312) 786-7428 or mollet@cboe.com if you have any questions regarding our comments.

Very truly yours,



Michael J. Mollet
Managing Director
CBOE Futures Exchange, LLC

¹ Regulation Systems Compliance and Integrity, 79 FR 72252, 72367 (Dec. 5, 2014).