



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: RIN 3038 – AE29, System Safeguards Testing Requirements for Derivatives Clearing Organizations; Proposed Rule

Dear Mr. Kirkpatrick,

LCH.Clearnet Limited, LCH.Clearnet SA and LCH.Clearnet LLC (together “LCH”) are each Derivatives Clearing Organizations (“DCOs”) registered with the Commodity Futures Trading Commission (the “CFTC” or “Commission”).

We welcome the opportunity to respond to this rulemaking¹ and commend the Commission on this initiative to strengthen the effectiveness of cybersecurity controls for DCOs. Strengthening cyber resilience is a global priority for financial market infrastructure (“FMI”) and establishing an enhanced common framework for applying the relevant Core Principles will ensure consistent practices across DCOs.

The Commission importantly recognizes the consistent, growing cybersecurity threat to the financial sector. We agree the proposed rules will provide clear and important benefits to DCOs and enhanced protection of the broader financial system. As discussed further in our comments below, LCH:

1. supports further strengthening of the relevant international standards and greater coordination across jurisdictions in enhancing system safeguards requirements for CCPs;
2. agrees that the proposed testing requirements are largely consistent with the relevant Core Principles and industry best practices;
3. recommends the CFTC consider certain factors when defining the date for compliance with the proposed rules.

International Coordination

We operate DCOs based in London, Paris and New York which requires direct supervisory engagement on system safeguards and cyber resilience topics with multiple regulators. This also results in the evaluation and application of multiple industry best practices and regulatory standards.

¹ System Safeguards Testing Requirements for Derivatives Clearing Organizations, 80 Fed. Reg. 80114 (Dec. 23, 2015) (“Proposed Rules”).

In our increasingly global and interconnected marketplace, we believe international coordination in applying consistent standards for system safeguards testing across jurisdictions is critical.

We commend CPMI-IOSCO's continued efforts to further strengthen harmonized standards for FMI cyber resilience programs.² We believe the leadership of the CFTC and regulatory counterparts in other jurisdictions will contribute to a stronger and more consistent international framework for CCPs. This is especially important in view of the upcoming international framework for CCP recovery and resolution rules, where non-default losses will be a key component.

Proposed Testing Requirements

We agree the proposed testing requirements will strengthen DCO system safeguards programs and are consistent with the relevant DCO Core Principles. We provide the following specific comments on the proposals:

Testing Frequency

Cybersecurity testing is crucial to efforts to strengthen cyber defences and maintain cyber resilience. Complete testing of all controls over a rolling two-year period is practical given the number of controls that may require testing. However, the engagement of independent contractors to perform two of the four required vulnerability tests will likely impose increased costs, especially for smaller DCOs. We believe an annual engagement of an independent contractor seems more practical and cost efficient, especially where it is more proportionate to the size and complexity of smaller DCOs.

Definition of "Independent contractor"

We believe the Commission should provide further guidance or a specific definition of the term "independent contractor" to maintain a consistent approach to be adopted by all DCOs. This clarity is important given the supply shortage of skilled professionals discussed further below.

Consideration of Costs and Benefits

We provide the following specific comments on the consideration of costs and benefits, particularly as it relates to setting the date for compliance with the final rules.

Defining the baseline for cost and benefit considerations

The Commission defines the baseline for the cost and benefit considerations as "*the set of requirements under the CEA and the Commission's regulation for DCOs.*"³ This incorporates both

² See CPMI-IOSCO, Consultative Report, Guidance on cyber resilience for financial market infrastructures, November 2015, available at <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD513.pdf>

³ Proposed Rules at 80125

generally accepted standards and industry best practices.⁴ The Commission's cost and benefit considerations also evaluate the proposal against the February 2015 DCR survey to which LCH provided a response of behalf of all three DCOs in the group.⁵

Due consideration must be given to defining a baseline consistent with multiple sets of periodically evolving best practices, both in the U.S. and abroad.⁶ Authorities in the U.S. or other jurisdictions may require different approaches to systems safeguards standards in certain areas.

We recommend that the CFTC consider the complexity created by multiple standards coming into effect in different major jurisdictions within the same timeframe. Although international DCOs will achieve compliance against the highest minimum standards, the lead time for building testing programs and supportive compliance controls to meet many sets of new standards could be longer for larger and more complex DCOs than for smaller, regional DCO operations.

Availability of skilled personnel

The complexity of attacks and need to manage technology, people and processes in support of cyber resilience programs continues to increase. At the same time, we recognize there remains an industry-wide shortage in the supply of skilled personnel from the board level down to operational staff. It is becoming increasingly difficult to get cyber risk management experience in the marketplace at reasonable cost.

This supply shortage of skilled professionals could increase costs directly and indirectly as a result of the proposed rules. For example, even the collection and presentation of relevant data for board or regulatory scrutiny can create a significant increase in resource uplift. We believe the Commission should take this into account in their analysis and in setting a date for compliance with the new rules.

Proportionality

We agree with the Commission's observation that it is important to factor in the size and complexity of a DCO's operations into the cost and benefit analysis.⁷ The Commission should consider the financial resources impact against the scale and complexity of the DCO. Again, this will be particularly important with respect to timing of the proposed rules becoming mandatory.

⁴ *Id.*

⁵ *Id.* at footnote 143.

⁶ In the European Union, the Network and Information Security (NIS) directive will soon enter into force. In France, the "Loi de Programmation Militaire" (article 22), which is a new framework of security requirements for all French critical operators, will also soon enter into force.

⁷ Proposed Rules at 80126.



LCH is grateful for the opportunity to comment on the proposed rulemaking and would be happy to provide further information related to the issues described in this letter at the Commission's request.

Sincerely,

A handwritten signature in black ink, appearing to read "Jonathan Jachym", written in a cursive style.

Jonathan Jachym
Head of North America Regulatory Strategy & Government Relations