National Futures Association

Leadership Perspectives – Resilience and Recovery and Cybersecurity Risks

CFTC Market Risk Advisory Committee

March 8, 2023

Background

In late January, a middle and back office service provider to FCMs, ION Cleared Derivatives (a subsidiary of ION Markets), experienced a significant outage due to a cybersecurity event. This incident was extremely serious and had an acute impact on several FCMs' ability to process trades, which impacted their business activities with customers and other FCMs.

We applaud the Futures Industry Association (FIA) in the immediate aftermath of the incident for assisting the industry in responding to this occurrence. Over several days, FIA held multiple daily videoconferences with numerous industry participants, including FCMs, other market participants, and U.S. and non-U.S. exchanges and clearinghouses to share information about this incident's disruptive impact on the global listed derivatives industry. The unified response to this incident facilitated the adoption of operational measures to mitigate its impact. Additionally, FIA's invitation for NFA and other regulators to join these videoconferences proved extremely helpful for us to understand the gravity of this cyber incident and to effectively provide appropriate regulatory relief from CFTC, NFA and CME Group requirements. As more information about this incident emerges, the industry and regulators should continue to fully evaluate this occurrence and what, if anything, we should do in response.

Over the years, NFA has worked with the industry and the CFTC to adopt requirements for our Members to establish and maintain:

- Business continuity and disaster recovery plans designed to implement recovery and resilience processes in the event of an emergency and significant business disruption (NFA Compliance Rule 2-38 and its related Interpretive Notice, *Business Continuity and Disaster Recovery Plan*, effective 2003);

- Practices reasonably designed to diligently supervise the risks of unauthorized access to or attack of their information technology systems, and to respond appropriately should an unauthorized access or attack occur (NFA Interpretive Notice, *NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs*, effective 2015); and

- A supervisory framework relating to third-party providers that perform regulatory functions to assist a Member in fulfilling its obligations pursuant to CFTC or NFA requirements (NFA Interpretive Notice, *NFA Compliance Rules 2-9 and 2-36: Members' Use of Third-Party Service Providers*, effective 2021).

Given that ION Cleared Derivatives was a third-party service provider, NFA believes a high-level description of the supervisory guidance provided in our 2021 Interpretive Notice (Notice) may be instructive to a future assessment of the potential operational and regulatory risks posed by third-party service providers.

NFA's Third-Party Service Provider Guidance

The Notice recognizes that a Member may fulfill, in part, its regulatory obligations by having a third-party service provider(s) or vendor(s) perform certain functions that would otherwise be undertaken by the Member itself to comply with NFA and CFTC Requirements. Historically, NFA Members have outsourced varied functions to third-party service providers and NFA understands that outsourcing may provide benefits to Members.

The Notice's primary purpose is to require each Member outsourcing regulatory functions[1] to adopt and implement a supervisory framework over its outsourcing function, which is designed to mitigate the risks associated with outsourcing. To assist Members with this framework, the Notice outlines minimum areas that should be addressed in a Member's supervisory framework and provides guidance on the types of processes a Member should implement, which include the following:

- *Initial Risk Assessment* – Requires a Member to determine whether a particular regulatory function is appropriate for outsourcing and, if so, evaluate the risks associated with outsourcing the function. The Notice directs Members to consider the risks related to information security, regulatory obligations and the impact on the Member, customers and counterparties if the service provider fails properly to carry out its obligations, and the location of the service provider and if it has the resources to meet its obligations;

- *Onboarding Due Diligence* – Requires a Member to conduct appropriate due diligence to ensure that a third party has the ability to successfully carry out the outsourced function in a manner that complies with regulatory requirements and to ensure that due diligence is commensurate with the risks (*e.g.,* holding critical or confidential data) associated with

[1] For example, these functions include, but are not limited to, those offering front, middle and back office services, swaps compression services, commodity pool fund administration services and anti-money laundering customer identification program services.

outsourcing a particular regulatory function. The Notice requires Members to execute a written agreement that, among other things, fully describes the scope of the services being performed;

- *Ongoing Monitoring* – Requires a Member to adopt a framework to monitor the third party's ability to carry out the outsourced function and identifies certain areas that should be reviewed. The Notice further provides guidance on senior management involvement and contract renewals;

- *Termination* – Requires a Member to continue to meet NFA and CFTC requirements, including those related to recordkeeping, after termination, and discusses special considerations relating to confidential information that may be in the third party's possession; and

- *Recordkeeping* – Requires a Member that engages a third party to carry out a regulatory function to maintain records to demonstrate that it has addressed the areas in the Notice in accordance with NFA Compliance Rules 2-10 and 2-49.

Conclusion

In the aftermath of the ION Cleared Derivative's incident, NFA is committed to working with the industry and CFTC to review if changes should be made to the Notice's supervisory guidance and any other requirements NFA currently has in place. Additionally, we recognize that, despite our Members' adherence to the Notice's guidance, future failures may occur, and it is extremely important for our Member firms to focus on the potential risks posed by third-party service providers and devise recovery and resilience processes in the event of an emergency and significant business disruption.