COVINGTON

Cybersecurity: Recent CFTC and NFA Activity

September 11, 2015

Futures and Derivatives

Commodity Futures Trading Commission (CFTC) Chairman Timothy Massad recently announced that cybersecurity in the futures and derivatives markets has become "perhaps the single most important new risk to market integrity and financial stability."[1] On September 9, 2015, Chairman Massad also announced that the CFTC was working on a rule proposal related to cybersecurity.[2] Following an industry roundtable on the topic earlier this year, Chairman Massad's statements, and recent CFTC commentary it would appear that the agency will issue a proposed cybersecurity rule, perhaps by the end of 2015.

Importantly, in August 2015 the National Futures Association (NFA), the self-regulatory organization responsible for the registration of certain market participants, requested that the CFTC review a new interpretive notice concerning NFA members' supervision of their information systems security programs.[3] The NFA's notice and, ultimately, a related proposed rule by the CFTC could result in a new approach for the CFTC's cybersecurity scheme. Current regulations generally emphasize a reactive approach to the issue, requiring business-continuity planning and post-attack recovery capacity, as opposed to specific attack-prevention techniques.

This advisory outlines the CFTC's existing cybersecurity framework and its anticipated changes throughout the remainder of 2015, as well as the NFA's recent proposal. Given Covington's CFTC and cybersecurity expertise, we remain well positioned to help market participants understand and implement existing and new rules.

Exchanges, Clearing Organizations, and Data Repositories

The CFTC currently regulates electronic trading platforms, such as designated contract markets (DCMs) and swap execution facilities (SEFs) by looking to existing industry practice. Since the passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), the CFTC has introduced additional prescriptive regulations related to system safeguards, which

[1] Timothy Massad, Chairman, CFTC, Keynote Address Before the Futures Industry Association Boca Conference (Mar. 11, 2015), available at: http://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-14.
[2] Timothy Massad, Chairman, CFTC, Keynote Address before the Beer Institute Annual Meeting (Sept. 9, 2015) (collectively with note 1, Massad Comments), available at: http://www.cftc.gov/PressRoom/SpeechesTestimony/opamassad-27 (stating "we are currently working on a proposal to make sure the private companies that run the core infrastructure under our jurisdiction… are doing adequate evaluation of these risks and testing of their own cybersecurity and operational risk protections.")
[3] National Futures Association Rule Submission Letter: Information Systems Security Programs - Proposed Adoption of the Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs (Aug. 28, 2015) (the NFA Cybersecurity Submission), available at: https://www.nfa.futures.org/news/PDF/CFTC/InterpNotc_CR2-9_2-36_2-49_InfoSystemsSecurityPrograms_Aug_2015.pdf.

require these platforms to maintain an operational risk and oversight program.[4] Generally, the CFTC has stated that participating platforms should structure their program according to "generally accepted standards and best practices" within their industries.[5] The CFTC requires DCMs and SEFs to maintain a business-continuity disaster recovery plan, to possess next-day trading and clearing capability following a disruption,[6] to conduct periodic systems testing, and to promptly report to the CFTC any cybersecurity incidents that could jeopardize a platform's systems operation. Such incidents can include mere targeted threats that do not ultimately impact business.[7] While the program must address system cybersecurity threats, the CFTC DCM regulations, last modified in 2012, use the word "cyber security" once.[8] The CFTC's regulation also extends to the DCM and SEF application processes, during which the CFTC asks applicants to provide detailed information regarding an applicant's technology architecture, information security program, and cybersecurity protections via a questionnaire and onsite inspection.[9]

Similarly, derivatives clearing organizations (DCOs) are required to adhere to "generally accepted standards and industry best practices with respect to the development, operation, reliability, security, and capacity of automated systems."[10] DCOs must maintain a risk management program in accordance with best practices, as well as a business-continuity plan and regular, periodic, and independent systems testing.[11] Systemically important derivatives clearing organizations, which are designated by the Financial Stability Oversight Council, are subject to similar standards, but must be able to resume operations within two hours.[12] DCOs must also notify the CFTC of "exceptional events," including a "cyber security incident."[13]

Lastly, the CFTC extends its general cybersecurity guidelines to address swaps data security. CFTC rules establish risk program, business-continuity plan, periodic systems testing, and incident reporting requirements for swap data repositories (SDRs). CFTC regulations also state that each SDR should coordinate its business-continuity plan with SEFs, DCMs, DCOs, and market participants "in a manner adequate to enable effective resumption of the [SDR's] fulfillment of its duties" should a wide-scale disruption occur.[14] Adequate coordination requires the maintenance of sufficient backup infrastructure and personnel to be able to resume operations even if physical, not merely operational, damage results from an attack. The CFTC's approach here also demonstrates the interconnectivity among regulated market participants.

---

[4] *See* CFTC Regulations 37.1400-37.1401 for SEFs and CFTC Regulations 38.1050-38.1051 for DCMs. For ease of presentation we have not cited Chapter 17 of the Code of Federal Regulation.
[5] *See* CFTC Regulation 37.1401; CFTC Regulation 38.1051.
[6] DCMs and SEFs that have been determined to be critical financial markets face heightened, same-day recovery requirements in the event of a wide-scale disruption. *See* CFTC Regulation 37.1401; CFTC Regulation 38.1051. However, the CFTC has not implemented additional regulations related to this determination. *Id*. and CFTC Regulation 40.9 (noting regulation is "reserved").
[7] *See* CFTC Regulation 37.1401; CFTC Regulation 38.1051.
[8] *Id*.
[9] For a detailed look at the CFTC's requested information, see the CFTC, Operational Capability Technology Questionnaire (2015), available at: http://www.cftc.gov/ucm/groups/public/@iodcms/documents/file/iodcm_octq.pdf.
[10] *See* CFTC Regulation 39.18(d).
[11] *See* CFTC Regulation 39.18.
[12] *See* CFTC Regulation 39.34(a) (discussing the recovery time objective). We would also note that many CFTC-regulated entities are also regulated by other agencies. Therefore, a market participant must also consider those rules in the context of any CFTC rules.
[13] *See* CFTC Regulation 39.18(g).
[14] *See* CFTC Regulation 49.24.

Market Participants and the CFTC

The CFTC's market participant cybersecurity rules for participants such as swap dealers (SDs), futures commission merchants (FCMs), commodity pool operators (CPOs), introducing brokers (IBs), commodity trade advisors (CTAs) and major swap participants (MSPs) reflect a similar regulatory approach that prioritizes incident response over incident prevention. For example, CFTC rules regulate market participant operations with an eye towards disaster recovery. CFTC requirements for FCMs, SDs, and MSPs are generally limited to the preparation of business-continuity plans, along with the related systems testing to ensure the participants' ability to swiftly recover from an attack. In some cases, the CFTC requires certain market participants to additionally prepare for third party cybersecurity risk. For instance, SDs and MSPs must account for potential interruptions to outside businesses that are necessary for SD and MSP functioning.[15] CPOs and CTAs are not subject to these additional requirements, as they serve less of a customer liquidity providing role.

Current CFTC market-participant cybersecurity regulation provides evidence of what could be a more preventative future approach. As part of its implementation of Dodd-Frank, the CFTC has mandated that market participants actively protect their customers' data. Specifically, CFTC Regulation 160.30 requires market actors to provide "administrative, technical and physical safeguards" to prevent the stealing of customer information by a cyber- agent.[16] Whether the CFTC will extend similar proactive safeguards from the realm of data security to that of business-operations security remains to be seen.

Market Participants and the NFA

NFA is responsible for the registration and oversight of SDs, FCMs, CPOs, IBs, CTAs and MSPs, which are referred to by NFA as Members. The NFA recently proposed the adoption of a new Interpretive Notice to several existing NFA compliance rules related to supervision. The NFA issues Interpretive Notices in order to "provide more specific guidance on acceptable standards for supervisory procedures."[17] The NFA Cybersecurity Submission notes that NFA "believes that Members should have supervisory practices in place reasonably designed to diligently supervise the risks of unauthorized access to or attack of their information technology systems, and to respond appropriately should unauthorized access or attack occur."[18] The NFA has not proposed prescriptive guidance because NFA Members differ in terms of type, size and complexity of operations. Therefore, NFA has proposed that Members "have an appropriate degree of flexibility to determine how best to diligently supervise information security risks" and has provided "general requirements relating to Members' information systems security programs (ISSPs) but leave the exact form of an ISSP up to each Member thereby allowing the Member flexibility to design and implement security standards, procedures and practices that are appropriate for their circumstances."

---

[15] See CFTC Regulation 23.603. We would also note that DCMs, SEFs, and DCOs have their own rules related to participant responsibilities with regard to testing and accessing their respective technology platforms.
[16] *See* CFTC Regulation 160.30.
[17] *See* NFA Cybersecurity Submission at 2.
[18] *Id.*

NFA's proposal focuses on an ISSP that covers the following:

- Written Program - a Member must adopt and enforce a written ISSP reasonably designed to provide appropriate safeguards, which is approved by an executive level official and briefed to a Member's board of directors or similar governing body;[19]
- Security and Risk Analysis - a Member must assess the threats to and the vulnerability of their enterprise, including identifying its "crown jewels" or most sensitive at-risk data;
- Deployment of Protective Measures Against the Identified Threats and Vulnerabilities - a Member must adopt safeguards (*e.g.*, complex passwords, firewalls, system back-ups, encryption software) and implement procedures to detect potential threats;
- Response and Recovery from Events that Threaten the Security of the Electronic Systems - a Member should consider an incident response plan that includes identifying key response team members, response procedures, and procedures to restore compromised systems and data; and
- Employee Training - a Member should provide education and training related to information security during new employee on-boarding and periodic training.[20]

NFA also proposes that the ISSP be monitored and reviewed on a regular basis to assess effectiveness, as well as manage the risks presented by third-party service providers and maintain records related to the ISSP.

Conclusion

Given Chairman Massad's recent statements, continued market commentary and recent NFA action, additional CFTC cybersecurity guidelines are forthcoming perhaps by the end of the year. Less clear is whether a new proposed rule will dramatically shift the existing regulatory landscape, which has prioritized post-incident response and recovery over proactive measures, which the NFA proposal demonstrates. This CFTC approach has remained despite our observation that preparing for incidents in advance typically minimizes the cost of incidents and better prepares clients to respond to cyber incidents.

Chairman Massad indicated in his March and September addresses that the expected rulemaking could emphasize cybersecurity systems testing.[21] This would build upon the current rules by taking existing regulations, such as those requiring a business-continuity plan, and adding an evaluative process, in which the industry's responses to existing regulations can be reviewed for effectiveness. Such a proposed rule would reinforce an already common and existing practice across multiple industries focusing on testing incident response—through tabletop exercises and other simulations—and business-continuity plans.

Whether or not this concept forms part of the future guidance, CFTC cybersecurity regulations remain in flux. Covington's expertise with CFTC regulation and cybersecurity prevention, investigation, and remediation means we remain well positioned to help market participants

[19] *Id*. at 5. In providing this requirement, NFA notes that members should look to several industry organizations for cybersecurity best practices and standards.
[20] *Id*. at 4-9.
[21] *See* Massad Comments, *supra* notes 1 and 2.

understand and implement any new rules in a manner practical to a market participant's business and respond to a cyberattack, if and when one should occur.

If you have any questions concerning the material discussed in this client alert, please contact the following members of either our Financial Institutions or Privacy & Data Security practice groups:

Stephen Humenik	+1 202 662 5803	shumenik@cov.com
David Fagan	+1 202 662 5291	dfagan@cov.com
Bruce Bennett	+1 212 841 1060	bbennett@cov.com
Ashden Fein	+1 202 662 5116	afein@cov.com
Ronald Hewitt	+1 212 841 1220	rhewitt@cov.com
James Kwok	+1 212 841 1033	jkwok@cov.com