Public Policy

November 23, 2015

Following a Regulatory Trend, CFTC Inches towards Cybersecurity Testing Requirements

By Andrew L. Caplan, Brian E. Finch and Elizabeth Vella Moeller

Commodity Futures Trading Commission (CFTC) Chairman Timothy Massad has recently stated that the CFTC may soon issue principles-based standards that would require certain CFTC-regulated entities to conduct penetration, vulnerability, and control testing of cybersecurity systems. This warning comes on the heels of recent activity by Federal and State financial regulators, who have been taking an increasingly active role in issuing specific cybersecurity requirements for regulated financial institutions. In light of the CFTC's current political make-up (two Democratic Commissioners who would apparently support CFTC-issued cybersecurity regulations and one Republican who may oppose them), it appears likely that we will see enhanced cybersecurity regulation of certain CFTC-regulated entities in the near term.

Background

In a series of public addresses this Fall, CFTC Chairman Timothy Massad has repeatedly stated that he expects the CFTC to soon (perhaps by the end of the year) take action to propose principles-based cybersecurity standards for major exchanges, clearinghouses, and swap data repositories.[1]

According to Chairman Massad's recent remarks, the CFTC's potential cybersecurity standards would ensure that clearinghouses, as well as other "core infrastructure" entities (*e.g.,* major exchanges and swap data repositories), are conducting adequate evaluations of cybersecurity risks and testing their cybersecurity and operational risk protections.

[1] *See e.g.,* Timothy G. Massad, Chairman, CFTC, Keynote Address before the Beer Institute Annual Meeting (Sep. 9, 2015); *see also* Timothy G. Massad, Chairman, CFTC, Keynote Remarks before the Risk USA Conference (Oct. 22, 2015); *see also* Timothy G. Massad, Chairman, CFTC, Keynote Remarks before the Futures Industry Association Futures and Options Expo (Nov. 4, 2015).

Per Chairman Massad's recent remarks, a CFTC cybersecurity regulatory proposal would apparently require certain regulated entities to engage in:

- Penetration testing (i.e., testing a network for vulnerabilities);
- Vulnerability testing (i.e., identifying, quantifying, and prioritizing vulnerabilities); and
- Control testing (i.e., testing of key controls to counteract these vulnerabilities).

These statements follow a March CFTC Staff Round Table on Cybersecurity and System Safeguards Testing, in which the CFTC sought industry and government agency feedback on what the CFTC's role should be to "add value" for regulated entities, in the context of cybersecurity. During this roundtable discussion, Chairman Massad noted that cybersecurity is the "most important single issue facing our markets today in terms of integrity and financial stability."[2]

Democratic CFTC Commissioner Sharon Bowen has also emphasized the need for enhanced CFTC regulation in the area of cybersecurity. According to Commissioner Bowen, CFTC registrants should be required to: (1) designate a central cybersecurity offer; (2) provide the CFTC with regular reports regarding the state of their cybersecurity programs; (3) report any material cybersecurity events to the CFTC promptly; and (4) sanction annual penetration testing by an independent auditor to ensure adoption of best practices.[3]

Both Chairman Massad's and Commissioner Bowen's remarks align with recent activity by the National Futures Association (the futures industry's self-regulatory organization), which, itself, has proposed principles-based cybersecurity standards for its members.[4]

It is worth noting that while the CFTC's Republican Commissioner, J. Christopher Giancarlo, may agree with Chairman Massad and Commissioner Bowen's expressed ends (protecting firms and the public against cybersecurity incidents), it is unclear whether he would agree with the means. In a recent keynote address, Commissioner Giancarlo supported Chairman Massad's position that cybersecurity is the most important single issue facing market integrity and financial stability, but at the same time, he disavowed any "top-down" approaches that would impose "dated mandates on firms that consume precious resources responding to last year's dramatic cyber-attack, causing them to miss the attack that will happen tomorrow…."[5]

Despite these remarks, in light of the CFTC's current make-up—two Democratic commissioners that actively support CFTC cybersecurity regulations and only one Republican commissioner to potentially vote against them—it appears likely that Chairman Massad's admonitions will come to fruition.

[2] *See* CFTC, Staff Roundtable on Cybersecurity and Systems Safeguard Testing (transcript), Washington D.C. (Mar. 18, 2015).

[3] *See* Sharon Y. Bowen, Commissioner, CFTC, Keynote Address before the ISDA North America Conference (Sep. 17, 2015).

[4] *See* National Futures Association, 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).

[5] *See* J. Christopher Giancarlo, Commissioner, CFTC, Keynote Address before the 2015 ISDA Annual Asia Pacific Conference (Oct. 26, 2015).

Activity by Other Financial Regulators

This "increased scrutiny" approach follows a recent trend among other financial regulators. Indeed, regulated financial institutions (including banks, capital markets participants, insurance companies, and other consumer finance firms) have lived under the general federal mandate that they adopt "reasonable" cybersecurity standards since the early 2000s, *viz*. the federal Gramm Leach Bliley Act and its implementing regulations.[6] However, most recently, both federal and state financial regulators have begun to add more color to what regulated firms must to do to ensure that they are implementing such "reasonable" protections.

For instance, on September 15, the Securities and Exchange Commission's Office of Compliance Inspections and Examinations ("OCIE") issued new examination priorities that registered broker-dealers and investment advisors should consider in implementing cybersecurity controls and procedures. These priorities include a review of a firm's

- Governance and risk assessment processes;
- Access rights and controls to systems or information;
- Data loss prevention standards;
- Vendor management standards;
- Employee training; and
- Incident response mechanisms.[7]

While these may just be examination priorities, an SEC-regulated entity would be ill advised to treat these exam procedures as mere "recommendations."

In an even more forceful move, on November 9, the New York Department of Financial Services (DFS) issued a letter to a long list of federal financial regulators (including the CFTC) outlining DFS's proposal for a new cybersecurity regulation.[8] DFS also indicated its hope that the letter would ultimately spark "regulatory convergence" among state and federal agencies on "new, strong cybersecurity standards for financial institutions."[9] The New York DFS's proposed regulations would include requirements that New York DFS-regulated entities implement:

- Required cybersecurity policies and procedures;
- Robust third-party service provider management controls;
- Required multi-factor authentication for certain sensitive information systems; and

[6] *See* 15 U.S.C. §§ 6801 *et. seq*.

[7] *See* SEC OCIE National Exam Program Risk Alert, vol. IV, issue 8 (Sep. 15, 2015).

[8] *See* Anthony J. Albanese, Acting Superintendent of Financial Services, New York Department of Financial Services, Letter to Financial and Banking Information Infrastructure Committee Members re Potential New NYDFS Cyber Security Regulation Requirements (Nov. 9, 2015).

[9] *See id*.

- Procedures to notify the DFS immediately of any cybersecurity incident that has a "reasonable likelihood of affecting the normal operations of the entity," among other requirements.

Consequently, if the CFTC were formally to issue a new cybersecurity mandate, it would be in keeping with the trend among other financial regulators.

Open Questions and Next Steps

Chairman Massad has stated that as "principles-based standards," the CFTC's mandate would likely outline the type of testing that is required; the CFTC would, however, "leave the detail of how to do the testing to the responsible firms."[10] While Chairman Massad's remarks would suggest that such principles-based standards would not require the use of any particular technology, it remains to be seen just how granular a CFTC proposed rule would be. It also remains to be seen who, exactly, will be covered by such requirements. Will there be an exception for smaller firms? Will firms that self-certify with other industry standards (perhaps those issued by the National Futures Association) enjoy any exemptions or safe harbors with respect to CFTC scrutiny? Would a CFTC regulation impose additional requirements, as Commissioner Bowen has suggested (for instance, requiring firms to appoint an employee with responsibility for cybersecurity)? The questions, among others, have yet to be answered.

Following Chairman Massad's remarks, as a likely next step, the CFTC may issue a Notice of Proposed Rulemaking, which would signal the CFTC's intent to issue a formal regulation on this issue. Although a formal rulemaking process would take some time to unfold, firms regulated by the CFTC should take note: tighter cybersecurity requirements are likely coming your way sooner, rather than later. CFTC-covered entities should be prepared to devote appropriate resources to comply with requirements for an independent third party to test and monitor safeguard systems, controls, and procedures that will protect the commodity futures trading system.

If you have any questions about the content of this alert please contact the Pillsbury attorney with whom you regularly work, or the authors below.

Andrew L. Caplan (bio)
Washington, DC
+1.202.663.8110
andrew.caplan@pillsburylaw.com

Brian E. Finch (bio)
Washington, DC
+1.202.663.8062
brian.finch@pillsburylaw.com

Elizabeth Vella Moeller (bio)
Washington, DC
+1.202.663.9159
elizabeth.moeller@pillsburylaw.com

[10] *See* Timothy G. Massad, Chairman, CFTC, Keynote Remarks before the Risk USA Conference (Oct. 22, 2015).

About Pillsbury Winthrop Shaw Pittman LLP

Pillsbury is a full-service law firm with an industry focus on energy & natural resources, financial services including financial institutions, real estate & construction, and technology. Based in the world's major financial, technology and energy centers, Pillsbury counsels clients on global business, regulatory and litigation matters. We work in multidisciplinary teams that allow us to understand our clients' objectives, anticipate trends, and bring a 360-degree perspective to complex business and legal issues—helping clients to take greater advantage of new opportunities, meet and exceed their objectives, and better mitigate risk. This collaborative work style helps produce the results our clients seek.