June 24, 2016

Christopher Kirkpatrick
Secretary of the Commission
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, N.W.
Washington, DC 20581

Via CFTC Web site: http://comments.cftc.gov

RE: RIN 3038-AD52 – Joint coalition comments in response to CFTC Proposed Regulation AT source code provisions

Dear Mr. Kirkpatrick:

The U.S. Chamber of Commerce (the "Chamber"), the Information Technology Industry Council ("ITI"), the Business Software Alliance, the International Swaps and Derivatives Association, the Futures Industry Association ("FIA"), the FIA Principal Traders Group, Modern Markets Initiative, and the Software & Information Industry Association write to you in strong opposition to the source code disclosure and retention requirements contained in the Commodity Futures Trading Commission's (the "CFTC") notice of proposed rulemaking on

Regulation Automated Trading ("Regulation AT")[1] and urge you to entirely eliminate these requirements from the final version of the rule.

In short, if not significantly amended, the proprietary source code provisions of Regulation AT will:

(1) compromise the established and expected due process rights of our members;

(2) increase the threat of "copycat" measures from other countries and contradict established U.S. policy on intellectual property disclosure;

(3) heighten the possibility of cyberattacks against government-mandated data repositories; and

(4) do little to assist the CFTC in its market surveillance activities.

While this letter is not an exhaustive listing of all of the issues of our associations may have with Regulation AT, we believe that it is important that the CFTC appreciate the broad-based opposition we have to Regulation AT's proprietary source code provisions.[2] We elaborate in additional detail below.

Mandating On-Demand Access to Proprietary Source Code Tramples Fundamental Due Process Rights and Attracts Similar Global Responses

Our chief concern with Regulation AT relates to the unprecedented, on-demand access that the CFTC would have to the proprietary source code of market participants engaged in algorithmic trading. Simply put, the proposed requirements force the disclosure of valuable intellectual property to the government based only on a showing that is akin to a document request. That type of requested access contradicts widely held expectations of due process associated with highly sensitive

---

[1] Commodity Futures Trading Commission, 80 Fed. Reg. 242 (proposed Dec. 17, 2015) (to be codified at 17 CFR Parts 1, 28, 40, et al).

[2] For additional detail, please see letter of March 16, 2016 to CFTC on Proposed Regulation AT source code provisions, available at the following link.

intellectual property—and, indeed, the legal protections that apply to any intellectual property in the U.S.

While the CFTC has recently acknowledged these concerns at a staff roundtable, there is no clear explanation as to why the CFTC could not use well-established U.S. judicial process to obtain access to proprietary source code data when needed. The CFTC and the DOJ have long used subpoenas to obtain access to non-public information and can continue to do so here. However, Regulation AT would provide an end-run around these important protections, eroding the important due process rights of these market participants.

Even more concerning is the precedent that the Regulation AT source code provisions would set, which may invite similar requirements in other countries. As recently as last year, the United States pushed back against a comparable proposal issued by the China Banking Regulatory Commission, which would have required American companies selling computer equipment to Chinese banks to turn over intellectual property and submit source code.[3] This action is also consistent with the U.S. government's policy against source code disclosure requirements in other contexts, as evidenced by previous opposition to proposed regulations issued by India's Department of Telecommunications relating to 2009-2010 Telecom Network Equipment Certification requirements, and by Korea's National Intelligence Service in 2005 relating to sales of information security software to Korean government agencies. Moreover, the signatories to the Trans-Pacific Partnership have also agreed not to require the transfer of, or access to, source code of software owned by a person of another party as a condition for the import, distribution, sale, or use of such software.[4]

These policy decisions from other parts of the U.S. government demonstrate a strong expression of U.S. Administration policy to defend the rights of intellectual property holders from unnecessary disclosure to third parties, including government

---

[3] Paul Mozur and Jane Perlez, *China Halts New Policy on Tech for Banks,* N.Y. TIMES, Apr. 16, 2015, *available at* http://www.nytimes.com/2015/04/17/business/international/china-suspends-rules-on-tech-companies-serving-banks.html?_r=0.

[4] See Article 14.17: Source Code, Trans-Pacific Partnership (ICT Annex), *available at* https://ustr.gov/sites/default/files/TPP-Final-Text-Electronic-Commerce.pdf.

entities. It also signals the extent to which the CFTC is a relative outlier compared to other financial services and capital markets regulators, and certainly with respect to other instrumentalities of the U.S. government. We believe that the CFTC should follow these decisions when finalizing Regulation AT, recognize the important of intellectual property to these firms, and respect the due process rights of its regulated entities.

Mandating On Demand Access to Proprietary Source Code is Inefficient and Will Not Assist the CFTC

Proprietary source code data is extremely difficult to understand without its developer, and simply viewing the source code on demand would not assist the CFTC in determining if automated trading contributed to a market-wide event. Participants at the CFTC's roundtable on June 10 noted that source code differs substantially from "books and records" requirements, in that proprietary source code does not solely provide information on instructions. Instead, it tells the story behind "why" and "how" a decision is made – much of which is impossible to understand without recreating a scenario event with the assistance of a developer.

Consequently, we fail to see how the CFTC's on demand access requirements will actually assist the agency in its market surveillance and investigative activities. In addition, the CFTC has not provided an estimate of the costs for hiring qualified developers that could actually analyze the proprietary source code, meaning that the CFTC currently does not know how much it would even cost to review information within its possession. We question the value of requesting on demand access to proprietary source code when the CFTC may not even have the resources to analyze it.

Regulation AT Increases the Potential for Cyberattacks and Threatens the Security of Proprietary Source Code

As proposed, Regulation AT requires automated trading firms to maintain source code repositories to manage source code access, maintain copies of production code (as well as logs of changes to production code), and include an audit trail to

determine who made changes to source code, under what circumstances, and why.[5] Such repositories must be available for inspection by the CFTC, the DOJ, and potentially third parties.

We strongly object to mandating automated trading firms to create source code repositories under the terms established by Regulation AT, especially when many companies already maintain such information. Moreover, establishing the same across-the-board requirement unintentionally makes those repositories "cyber targets," giving hackers and others a precise location for obtaining an automated trading firm's most valuable intellectual property.

Moreover, there is substantial reason to believe that proprietary source code data would not be safe in a government-mandated repository or in the hands of the Federal government. In the past year, we have seen cyberattacks against the Internal Revenue Service,[6] the Office of Personnel Management,[7] the Federal Deposit Insurance Company,[8] and the Board of Governors of the Federal Reserve.[9] Even the CFTC suffered its own data breach in June of 2012, risking the security of its employees' social security numbers.[10] Given how incredibly valuable proprietary source code data would potentially be in the hands of a hacker, we believe that these data breaches are enough reason for the CFTC to eliminate this element of Regulation AT.

Conclusion

While we appreciate the CFTC's need for timely access to data in order to fulfill its market surveillance mission, the proprietary source code requirements of

---

[5] See *supra* note 1 at p. 78824.

[6] Stephen Dinan, *IRS hit by cyberattack, thousands of taxpayers' information stolen*, THE WASHINGTON TIMES, May 26, 2015, *available at* http://www.washingtontimes.com/news/2015/may/26/irs-hit-cyberattack-thousands-taxpayers-informatio/.

[7] Julianne Pepitone, *Federal Data Breach: Can the Government Protect Itself From Hackers?*, NBC NEWS, Jun 5, 2015, *available at* http://www.nbcnews.com/tech/security/federal-data-breach-can-government-protect-itself-hackers-n370556.

[8] Joe Davidson, *FDIC cyberattacks included hit on former chairwoman's computer*, THE WASHINGTON POST, May 11, 2016, *available at* https://www.washingtonpost.com/news/powerpost/wp/2016/05/11/fdic-cyberattacks-included-hit-on-former-chairmans-computer/.

[9] David Murphy, *House Committee Investigates Federal Reserve Cyber-Attacks*, PC MAG, Jun 4, 2016, *available at* http://www.pcmag.com/news/344991/house-committee-investigates-federal-reserve-cyber-attacks.

[10] Silla Brush, *CFTC Data Breach Risks Employees' Social Security Numbers*, BLOOMBERG NEWS, June 25, 2015, *available at* http://www.bloomberg.com/news/articles/2012-06-25/cftc-data-breach-risks-employees-social-security-numbers.

Regulation AT are a bridge too far. By mandating on demand access to proprietary source code and the development of source code repositories, the CFTC not only compromises established due process rights—it also adopts policy in direct contradiction to other agencies of the U.S. government and increases the risk of cyberattack, all while not providing any tangible benefit to the CFTC. Consequently, we believe that the proprietary source code provisions of Regulation AT should be eliminated in their entirety.

<div align="center">

Sincerely,
BSA | The Software Alliance
Information Technology Industry Council
International Swaps and Derivatives Association
Futures Industry Association
FIA Principal Traders Group
Modern Markets Initiative
Software & Information Industry Association
U.S. Chamber of Commerce

</div>