March 16, 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 - ITI and U.S. Chamber of Commerce comments in response to CFTC Proposed Regulation AT source code provisions

Dear Mr. Kirkpatrick:

The Information Technology Industry Council (ITI), the U.S. Chamber of Commerce, and our member companies appreciate the opportunity to offer input on the Commodity Futures Trading Commission (CFTC)'s Notice of proposed rulemaking, 17 CFR Parts 1, 38, 40, and 170, Regulation Automated Trading ("Regulation AT"), as published in the Federal Register on December 17, 2015.

ITI is the global voice of the technology sector. As an advocacy and policy organization for the world's leading innovation companies, ITI navigates the relationships between policymakers, companies, and non-governmental organizations, providing creative solutions to advance the development and use of technology around the world. The U.S. Chamber of Commerce is the world's largest federation of businesses and associations, representing the interests of more than three million U.S. businesses and professional organizations of every size and in every economic sector. Collectively, our associations' members employ millions of workers across all sectors of the economy.

We support the CFTC's desire to promote best practices and regulatory standards for automated trading, but we have serious concerns that certain elements of the proposed regulation may unintentionally undermine the CFTC's express goal of reducing risk, and our shared goals of creating and maintaining a secure operating environment for automated trading, and improving the cybersecurity of the global digital infrastructure more generally. The proposed regulation thus may frustrate the intent of the CFTC and harm businesses at the same time. We outline our specific concerns below.

Our concerns focus on Regulation AT's source code provisions

We are particularly concerned with, and focus our comments on, the source code provisions of proposed Regulation AT – primarily contained in § 1.81 - Standards for Development, Monitoring, and Compliance of Algorithmic Trading Systems.

While we have little doubt that automated trading firms and other financial market participants will separately raise concerns with respect to proposed Regulation AT's source code provisions, the primary aim of our comments is to illuminate for the CFTC the broad potential negative impacts of the rule on not only the companies targeted by the rule, but a wide array of technology and other companies – both in the U.S. and abroad. In our view, the source code provisions of proposed Regulation AT are fundamentally flawed on at least two counts:

- Requiring companies to turn over proprietary source code on demand to government entities without due process sets a dangerous global precedent.
- Mandating that any companies (automated trading or otherwise) maintain government accessible source code repositories is insecure, inefficient, and likely ineffective.

Requiring companies to turn over proprietary source code to government on demand without due process sets a dangerous global precedent out of step with global norms

Requiring source code be turned over to government on demand sets a bad global precedent. Currently, the CFTC has the authority to issue subpoenas in enforcement cases, and the Department of Justice (DOJ), of course, possesses subpoena power as well. Source code represents the valuable intellectual property (IP) of companies. In the case of automated trading firms, the algorithms comprising their IP is likely the most valuable property they own. Protection of private property (and especially IP) is one of the distinguishing successes of the U.S. judicial system. When private property rights are threatened, the incentive for companies to innovate evaporates.

Simply stated, U.S. authorities should be required to obtain a subpoena to access companies' source code or other IP. We are struggling to understand the rationale of proposed Regulation AT's requirement that companies maintain source code repositories that must be turned over to the CFTC or DOJ on demand, without any due process whatsoever. Removing the current due process bar of a subpoena and empowering the CFTC or DOJ to gain unfettered access to the lifeblood of a business makes little sense, and even less when we consider the precedent Regulation AT sets. Such an arrangement not only raises concerns about data security risks and abusing the access to sensitive information, but establishes a United States federal policy that could serve as an "attractive nuisance" for others, impacting both how other federal agencies and other countries define policies and best practices in this area.

To the extent that the CFTC gains access to source code as prescribed by Regulation AT, we expect the SEC and other regulators to follow suit and similarly demand the authority to easily

access such information. While it would be bad enough if turning over source code "on demand" becomes the norm in the U.S., even more alarming is the precedent this may set globally, where the prospective damage to companies' IP rights is potentially magnified in countries without strong IP protections.

Mandating source code disclosure is bad cybersecurity policy, and out of step with global norms. Ultimately, it is important to examine proposed Regulation AT and its source code disclosure and escrow requirements in their broader context. As a preliminary matter, doing so requires recognizing that cybersecurity is a global issue, requiring global solutions to be truly effective. Financial markets, too, are increasingly global in nature, and interconnected, with global systems playing an important role for financial markets and institutions to promote security. Cyber risks transcend national borders, so countries – through their governments and private sector institutions – need to work together to develop safeguards that protect the integrity of global financial markets, and the global digital infrastructure more generally.

As a consequence, the financial sector is subject to a significant and diverse number of laws, regulations and examination standards related to cybersecurity that, together, broadly reflect an emerging international consensus regarding what cybersecurity standards are most effective.

Specifically, requirements to disclose source code are problematic in a globalized economy which is one reason they are not a feature of prevailing rules and regulations in other markets. Indeed, the United States government has consistently pushed back on source code disclosure requirements globally, including most recently on a 2015 proposal by the China Banking Regulatory Commission (a proposal since suspended). Internationally-accepted standards on software and IP licensing typically preclude banks from disclosing or holding third party IP in escrow without permission from the owners (or licensors) of that IP. Such disclosure would expose firms to unquantifiable financial risk from litigation and IP actions by software and IP licensors for breach of standard controls and contractual provisions protecting supplier IP.

Further, cybersecurity risks and the technology that mitigate them shift faster than regulations and standards can respond. As a consequence, policies that require specific technology requirements, detailed technical reviews or other processes by regulators will be reactive to the environment and to adversaries that seek to take advantage of vulnerabilities. In addition, written regulations and prescriptive standards become quickly outdated as cyber risks and the technology to address them evolve and create obstacles to protecting financial institutions and their clients. As recognized by the approaches taken by policymakers in a number of markets, effective regulations go beyond assessing whether an institution is compliant with a particular standard and instead seek to ensure that sufficient people, processes, and technology are in place to manage risks.

Mandating that companies maintain government accessible source code repositories is inefficient, insecure, and likely ineffective

Mandating that companies maintain government accessible source code repositories creates an automated trading environment that is less secure. As stated at the outset of proposed Regulation AT, one of the CFTC's primary purposes in promulgating the proposed rules was to "adopt a comprehensive approach to reducing risk … in automated trading" including risk controls and other safeguards.[1] Unfortunately, the proposed rule would have the opposite of its intended effect of reducing risk, by exposing automated trading firms' proprietary information to increased security risks, and potentially introducing security risks to U.S. markets more broadly.

Proposed § 1.81(a)(1)(vi) requires automated trading firms to "maintain a source code repository to manage source code access, persistence, copies of production code, and changes to production code … including an audit trail of material changes to source code that would allow automated trading firms to determine, for each such material change: who made it; when they made it; and the coding purpose of the change."[2] Automated trading firms must also make such source code repositories available for inspection, by the CFTC, the DOJ, and potentially third parties.[3]

The requirements of § 1.81(a)(1)(vi) thus create incremental insecurity in at least two respects. First, mandating that companies store source code as set forth in the proposed rule – in government accessible repositories - does the equivalent of painting a cyber target on these repositories; the known availability of valuable intellectual property is likely to incentivize hackers of all stripes to increase the number of cyber attacks launched against such repositories, likely resulting in an overall automated trading environment that is less secure and more difficult to defend from a cybersecurity standpoint.

Second, given the proposed rule seems to contemplate government access to automated trading firms' source code "on demand," without any legal process whatsoever, an untold amount of these companies' proprietary source code will likely wind up residing on the servers of U.S. government agencies. There are significant and well-founded concerns regarding the ability of the federal government to maintain the confidentiality and security of source code that may come into their possession as a result of this proposed regulation. As Commissioner J. Christopher Giancarlo pointed out in Appendix 4 to Regulation AT, "the federal government has a poor track record of keeping sensitive information secure from cyberattacks and other data breaches."[4] So any proposal that opens the door to placing private companies' source code on

[1] Commodity Futures Trading Commission, 80 Fed. Reg. 242 (proposed December 17, 2015) (to be codified at 17 CFR Parts 1, 28, 40, et al), p. 78824.
[2] *Id.* at 78847-48.
[3] *Id.* at 78938.
[4] *Id.* at 78947.

government servers seems a risky proposition at best. Any data breach of this information would be devastating for such companies and, potentially, for the security and orderly operation of U.S. financial markets. As Commissioner Giancarlo further opined, "Imagine the harm that could be caused to U.S. financial markets, if cyber terrorists or other belligerents were able to get their hands on this technology the same way some of the U.S.' most important industrial, military and other sensitive data have been hacked."[5]

Incidents that disrupt the integrity of the automated trading infrastructure not only impact the individual operations of designated contract markets, but also undermine the confidence of consumers and investors, potentially threatening the stability of global financial markets and systems. As a consequence, effectively addressing cyber risks in automated trading environments and the financial sector more broadly is critical to maintaining public confidence and mitigating financial risks. Requirements to escrow source code for several years, and make it available on demand without any legal showing whatsoever, are contrary to these goals.

Mandating that companies maintain source code repositories is costly and inefficient. The source code provisions of Regulation AT overlook the costs to companies of implementing the rule, as well as the resource drain on government agencies to process any information gained, relative to any perceived benefits. First, companies would have to incur substantial overhead to manage source code in the prescriptive manner required by the proposed regulation, including to maintain redundant copies of perhaps millions of lines of code, providing a detailed "audit trail" of all material changes to firms' source code, and of course paying to secure such statutorily required copies of and logs regarding such code. The costs of Regulation AT's source code requirements on companies will be particularly pronounced for smaller firms who are the most likely innovators in the automated trading space; the result is the proposed regulation may potentially act as a market entry barrier for these most innovative of firms.

Second, it is highly unlikely that government regulators possess the know-how to understand companies' source code, in the event it is turned over to them as envisioned pursuant to Regulation AT. Thus, implementation of the regulation would require the government to expend a substantial amount of resources to develop sufficient enough expertise to understand even limited portions of the source code captured by the broad sweep of the proposed regulation.

However, to potential thieves of automated trading firms' intellectual property, the cost-benefit analysis is absolutely worth significant investment of time and resources. It is perhaps a cybersecurity cliché to point out that, while defenders need to be right all of the time in order to protect valuable intellectual property or other proprietary information subject to cyber attacks, attackers or hackers only need to be right once to score a major payday; however, this is a cliché because it's unfortunately true. The potential cost of Regulation AT's source code

[5] *Id.*

provisions, in terms of jeopardizing the sanctity of private intellectual property in the United States, is potentially immeasurable.

The source code requirements will likely be ineffective, given their presumed underlying goals. While the precise rationale behind the source code repository requirements is muddled at best, presumably one driver is to help the CFTC reconstruct market events after the fact. Simply stated, having unfettered access to the source code will not help the CFTC achieve this goal. This is because analyzing source code alone, in a vacuum, will reveal little if anything about a given underlying market event. Automated trading algorithms make trading decisions based on various market data points - decisions cannot be inferred without understanding the context – *i.e.*, the information the algorithm was processing as well.

Conclusion

While we appreciate the CFTC's goals of promoting best practices and regulatory standards for reducing perceived risks around automated trading, we are concerned that the source code provisions of Regulation AT may have the opposite of their desired effect, unintentionally undermining the CFTC's express goal of reducing risk, and our shared goals of creating and maintaining a secure operating environment for automated trading and improving the cybersecurity of the global digital infrastructure more generally. We are also particularly concerned about the negative precedential effects this rule could have on regulated entities in the U.S. and technology and other companies globally.

As a consequence, we respectfully urge CFTC to issue a revised Regulation AT that respects companies' valuable IP and due process rights, is consistent with sound cybersecurity risk management principles, and is in sync with global practices regarding source code disclosure.

We thank the CFTC for the opportunity to provide comments on proposed Regulation AT, and are available upon request to further to address these issues and to answer any questions.

Respectfully,

John S. Miller
Vice President, Global Cybersecurity and Privacy Policy,
ITI - Information Technology Industry Council

Amanda E. Eversole
President, Center for Advanced Technology & Innovation Policy,
Senior Vice President, Center for Capital Markets Competitiveness,
& Senior Vice President, U.S. Chamber of Commerce