



May 1, 2017

**Via Website Submission**

Christopher Kirkpatrick  
Secretary of the Commission  
Commodity Futures Trading Commission  
Three Lafayette Centre  
1155 21<sup>st</sup> Street, NW  
Washington, DC 20581

**Re: RIN 3038-AD52; Supplemental Proposal on Regulation AT**

Dear Mr. Kirkpatrick:

Managed Funds Association<sup>1</sup> (“**MFA**”) and the Alternative Investment Management Association<sup>2</sup> (“**AIMA**”) (together, the “**Associations**”) are pleased to submit comments to the Commodity Futures Trading Commission (the “**CFTC**” or the “**Commission**”) on its supplemental notice of proposed rulemaking on Regulation AT (“**Supplemental Proposal**”).<sup>3</sup> We have been engaged with the Commission for years on ways to further strengthen the regulation of electronic trading, including the 2013 Concept Release on Risk Controls and System Safeguards for Automated Trading and the notice of proposed rulemaking on the regulation of automated trading (“**NPRM**”) (together with the Supplemental Proposal, “**Regulation AT**”).<sup>4</sup> As fiduciaries

---

<sup>1</sup>Managed Funds Association (“**MFA**”) represents the global alternative investment industry and its investors by advocating for sound industry practices and public policies that foster efficient, transparent, and fair capital markets. MFA, based in Washington, DC, is an advocacy, education, and communications organization established to enable hedge fund and managed futures firms in the alternative investment industry to participate in public policy discourse, share best practices and learn from peers, and communicate the industry’s contributions to the global economy. MFA members help pension plans, university endowments, charitable organizations, qualified individuals and other institutional investors to diversify their investments, manage risk, and generate attractive returns. MFA has cultivated a global membership and actively engages with regulators and policy makers in Asia, Europe, North and South America, and many other regions where MFA members are market participants.

<sup>2</sup> AIMA, the Alternative Investment Management Association, is the global representative of the alternative investment industry, with more than 1,700 corporate members in over 50 countries. AIMA works closely with its members to provide leadership in industry initiatives such as advocacy, policy and regulatory engagement, educational programmes, and sound practice guides. Providing an extensive global network for its members, AIMA’s primary membership is drawn from the alternative investment industry whose managers pursue a wide range of sophisticated asset management strategies. AIMA’s manager members collectively manage more than \$1.5 trillion in assets.

<sup>3</sup>81 *Fed. Reg.* 85,334 (Nov. 25, 2016); *see also* CFTC notice of proposed rulemaking on Regulation AT, 80 *Fed. Reg.* 78,824 (Dec. 17, 2015) (hereinafter “**NPRM**”).

<sup>4</sup> *See, e.g.*, letter from Stuart J. Kaswell, Executive Vice President & General Counsel, MFA, to Melissa D. Jurgens, Secretary, CFTC, dated December 11, 2013, on the Concept Release on Risk Controls and System Safeguards for Automated Trading Environments, available at: <https://www.managedfunds.org/wp-content/uploads/2013/12/MFA-CFTC-concept-rel-final-12-11-13.pdf>; letter from Stuart J. Kaswell, Executive Vice President & General Counsel, MFA, to Christopher Kirkpatrick, Secretary, CFTC, dated March 16, 2016, on proposed regulation automated trading

to investors and as market participants, our members have a keen interest in safeguarding the safety and soundness of U.S. derivative markets. Those concerns include the usability, affordability, efficiency and liquidity of these markets for the U.S. economy and for the hedging and risk management purposes for which these markets serve for market participants globally.

The Associations appreciate that the CFTC and its staff have attempted to incorporate comments it received on the NPRM into the Supplemental Proposal; however, we remain strongly concerned that the underlying framework of Regulation AT is flawed. As such, we believe a fundamental revision is necessary, and respectfully urge the Commission to abandon Regulation AT, as repropoed.

Contrary to the Commission's intention, we believe that, as drafted, Regulation AT would create new risks, impose inefficient and ineffective requirements and burdens on the CFTC, designated contract markets ("DCMs"), and market participants. This is because Regulation AT proposes to apply a very prescriptive, unnecessary, one-size-fits-all regulatory framework on many different types of market participants. For example, the definitions under Regulation AT continue to be so broad that almost all trading by all market participants will be needlessly swept within the scope of Algorithmic Trading and Direct Electronic Access. Subjecting all market participants to Regulation AT for the use of third-party Algorithmic Trading systems puts them in the untenable position of being responsible for systems and processes for which they have no means to assess regardless of their technical expertise. We also are concerned that in prescribing rigid controls and standards, Regulation AT does not provide enough flexibility for the markets and market participants to innovate or adjust their firms' controls or processes, as deemed appropriate or necessary to address new technologies and circumstances in the future. In addition, we think that Regulation AT is inconsistent with the objectives of Acting Chair Giancarlo's Project KISS—Keep It Simple Stupid—initiative.<sup>5</sup>

We believe the Commission should modernize regulatory oversight of automated trading by adopting targeted regulatory solutions to address marketplace risk. In doing so, we respectfully urge the Commission to develop a regulatory framework that establishes baseline risk controls among "gatekeepers" such as DCMs and futures commission merchants ("FCMs") or clearing firms to address the risk of market disruption. Any additional regulations should be integrated into

---

(hereinafter "MFA March 16, 2016 Letter"), attached as **Appendix A** and available at: <https://www.managedfunds.org/wp-content/uploads/2016/03/MFA-RegAT-Letter-final.pdf>. See also, letter from Stuart J. Kaswell, Executive Vice President & General Counsel, MFA, to Christopher Kirkpatrick, Secretary, CFTC, dated June 24, 2016, in connection to the CFTC Roundtable on June 10, 2016, available at: [https://www.managedfunds.org/wp-content/uploads/2016/06/MFA-Reg-AT-Roundtable.final\\_6.24.16.pdf](https://www.managedfunds.org/wp-content/uploads/2016/06/MFA-Reg-AT-Roundtable.final_6.24.16.pdf); and letter from Asset Management Group of SIFMA, FIA, FIA Principal Traders Group, ISDA, and MFA, to Christopher Kirkpatrick, Secretary, CFTC, dated June 24, 2016, regarding the public staff roundtable on elements of Regulation Automated Trading, (hereinafter, the "**June 24, 2016 Group Letter**"), available at: <https://www.managedfunds.org/wp-content/uploads/2016/06/REG-AT-Roundtable-Group-Comment-Letter-062416.pdf>.

<sup>5</sup> "CFTC: A New Direction Forward," Remarks of Acting Chairman J. Christopher Giancarlo before the 42<sup>nd</sup> Annual International Futures Industry Conference in Boca Raton, FL March 15, 2017 (hereinafter "**Giancarlo Boca Remarks**," available at: <http://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-20>).

the existing regulatory framework. Attempting to “modernize” oversight by simply layering another level of regulation on market participants and subjecting them to multiple DCM oversight creates an unwieldy and inefficient regulatory regime. Finally, we strongly concur with Acting Chair Giancarlo in noting that, in our experience, the Commission has adequate authority through the subpoena process to seek Algorithmic Trading Source Code and should continue to rely on this authority rather than circumvent an intellectual property owner’s right to due process of law.<sup>6</sup>

## I. EXECUTIVE SUMMARY

The Associations respectfully urge the Commission to abandon Regulation AT, as repropounded. Instead, the Commission should:

- **Reduce electronic trading risk** by implementing a risk control framework at the marketplace “gatekeeper” levels—DCMs and executing FCMs or clearing firms.
- **Build on the existing regulatory framework** to oversee registrants, such as CTAs and CPOs, rather than layer on an additional and separate system of automated trading requirements.

The Associations also provide specific comments to the Supplemental Proposal to illustrate some of our general concerns with it.

If the Commission determines to proceed with adopting Regulation AT, we believe it must:

- **Narrow the scope of Regulation AT** and use more precise definitions.
- **Adopt a principles-based approach** to regulation of automated trading that will allow market participants to tailor controls to suit their firms’ operations and risks.
- **Adopt a preservation requirement for Algorithmic Trading Source Code** and use the existing subpoena process for accessing Algorithmic Trading Source Code.
- **Adopt greater regulatory protections** for the treatment of Algorithmic Trading Source Code and other intellectual property.
- **Work with financial technology companies** to address how regulation can most effectively address new technologies and promote safer and more efficient markets, without subjecting market participants to Regulation AT for use of third-party algorithmic trading systems.

---

<sup>6</sup> See Statement of Dissent by Commissioner J. Christopher Giancarlo Regarding Supplemental Notice of Proposed Rulemaking on Regulation Automated Trading, November 4, 2016 (hereinafter “**Giancarlo Statement of Dissent**”), available at: <http://www.cftc.gov/PressRoom/SpeechesTestimony/giancarlostatement110416>.

## II. GENERAL COMMENTS

The Associations believe that Regulation AT, as drafted, is fundamentally flawed and misdirected. Regulation AT creates a complex and elaborate regulatory framework, which we believe will be burdensome for both regulators and market participants. We remain concerned that the definitions under Regulation AT are overly broad and are likely to quickly become outdated. In that regard, we believe that the trigger for the application of Regulation AT should not be tied to a market participant's own algorithmic trading activity. As market participants continue to innovate and automate functions that were once performed manually, we believe standardized risk controls are likely to be more efficient than focusing on individual trading firms and algorithms. We believe the solution to effective and timeless oversight is to implement a risk control framework at the gatekeeper levels (DCMs and executing FCMs or clearing firms), and for market participants to implement risk controls appropriate to their individual trading activities.

The general infrastructure for addressing marketplace risk at the gatekeeper level already exists. If the Commission believes more needs to be done, it should focus on establishing baseline sets of pre-trade risk and other controls at the DCMs and the executing FCM or clearing firms. As the Associations' members are CTAs and CPOs, subject to regulation by the CFTC, National Futures Association ("NFA") and the Securities and Exchange Commission, our letter focuses on what we believe is appropriate for this set of registrants.

We continue to believe that the Commission should use the existing regulatory framework to oversee CTAs and CPOs, rather than layer on an additional and separate system of requirements without first considering whether the existing framework provides sufficient oversight.<sup>7</sup> To the extent that the Commission believes it needs more information from CTAs or CPOs, or that these registered entities need enhanced controls, we would strongly urge the Commission to direct the NFA to amend its Annual Questionnaire. From data the NFA collects through its Annual Questionnaire, the Commission would be able to assess whether additional requirements are necessary to address risk concerns. If, after thorough review, the Commission determines that additional controls and documentation requirements are in fact needed, we believe the Commission should use the existing regulatory framework and amend its Part 4 regulations to address CTA/CPO operational systems risk concerns related to algorithmic trading in a manner suited for CTA and CPO businesses and operations. This sort of targeted approach would more precisely achieve the Commission's goals at lower cost.

Accordingly, we strongly recommend that the Commission abandon Regulation AT as proposed, and instead to: (1) reduce electronic trading risk by implementing a risk control framework at the marketplace gatekeeper levels—DCMs and executing FCMs or clearing firms; and (2) build on the existing regulatory framework, as necessary, to oversee registrants, such as CTAs and CPOs.

---

<sup>7</sup> *Id.*

### III. SPECIFIC COMMENTS ON THE SUPPLEMENTAL PROPOSAL

To the extent the Commission determines to proceed with the Regulation AT, we provide below some specific comments on the Supplemental Proposal for the Commission's consideration and to illustrate our concerns with Regulation AT.

We have strong concerns with the Supplemental Proposal as it does not address our primary concern with Regulation AT, which is that it implements a one-size-fits-all approach to regulating automated trading—that it does not make adequate distinctions among different types of market participants, nor does it recognize the different business structures, business models and operational sizes of market participants. CTAs and CPOs employ diverse investment strategies, ranging from entirely manual, partially-automated, to fully-automated. While most CTAs and CPOs use third-party execution algorithms, some develop and build their own proprietary execution algorithms.<sup>8</sup> We believe that Regulation AT would be very burdensome for CTAs and CPOs because it prescribes measures which are not appropriately tailored for the individual business or strategies of CTAs or CPOs.<sup>9</sup> In addition, the requirements for a CTA or CPO that uses a third-party execution algorithm are so prescriptive and detailed that a CTA or CPO cannot meaningfully conduct due diligence on the accuracy and sufficiency of a certification by a third-party vendor to satisfy itself that it is in compliance with Regulation AT. As such, the regulatory and compliance costs associated with Regulation AT will significantly raise the barriers to trading commodity interests for many market participants and likely lead to decreased liquidity in the exchange-traded derivatives markets. It would be a shame if some of the benefits of increased technology in the derivatives markets—the linkages, increased participation, and efficiency—are undermined by misguided regulation that makes these markets less accessible.

In this respect, we think the Commission should narrow the focus and scope of Regulation AT to exclude CTAs and CPOs; and direct NFA to collect information from CTAs and CPOs through its Annual Questionnaire on operational systems risk controls related to algorithmic trading.

---

<sup>8</sup> See June 24, 2016 Group Letter at p. 14 (discussing how FCM customers access markets).

<sup>9</sup> See MFA March 16, 2016 Letter, Appendix A.

## A. Volume Threshold Test for AT Person & Regulation AT Definitions

### 1. The AT Person Framework

We appreciate that the Supplemental Proposal attempts to narrow the definition of AT Person<sup>10</sup> by incorporating a Volume Threshold Test.<sup>11</sup> The Supplemental Proposal, however, does not address an underlying problem with Regulation AT which is that it continues to regulate all automated trading functions in the same manner. This, in part, is because the Supplemental Proposal fails to amend the definition of Algorithmic Trading<sup>12</sup> and the term, as defined, covers

---

<sup>10</sup> See Supplemental Proposal at 85,391. § 1.3(xxxx) *AT Person*. (1) This term means any person registered or required to be registered as a—

(i) Futures commission merchant, floor broker, swap dealer, major swap participant, commodity pool operator, commodity trading advisor, or introducing broker that

(A) engages in Algorithmic Trading on or subject to the rules of a designated contract market; and

(B) with respect to purchases or sales of any commodity for future delivery, security futures product, or swap, or any commodity option authorized under section 4c of the Act, satisfies, or has satisfied, the volume threshold test set forth in (x)(2) of this section; provided, however, that if an AT Person does not satisfy such volume threshold test for two consecutive semi-annual periods, as outlined in (x)(2) of this section, then such person shall no longer be considered an AT Person; or

(ii) Floor trader as defined in (x)(1)(iii) of this section.

(2) (i) A person who does not satisfy the conditions of (xxxx)(1) of this section may elect to become an AT Person, provided that such person:

(A) registers as a floor trader as defined in (x)(1)(ii) of this section; and

(B) submits an application for membership in at least one registered futures association pursuant to Commission regulation 170.18.

(ii) A person who elects to become an AT Person pursuant to (xxxx)(2)(i) of this section shall comply with all requirements of AT Persons pursuant to Commission regulations.

<sup>11</sup> See Supplemental Proposal at 85,391. Under § 1.3(xxxx), an AT Person satisfies the volume threshold test (“**Volume Threshold Test**”) under paragraph (x)(2), if such person trades an aggregate average daily volume of at least 20,000 contracts for such person’s own account, the accounts of customers, or both where:

(i) Such person shall calculate the aggregate average daily volume across all products and on the electronic trading facilities of all designated contract markets where such person trades;

(ii) Such person shall calculate the aggregate average daily volume for each January 1 through June 30 and July 1 through December 31 period, based on all trading days in the respective period; and

(iii) For purposes of calculating the aggregate average daily volume, such person shall aggregate its own trading volume and that of any other persons controlling, controlled by or under common control with such person.

<sup>12</sup> See NPRM at 78,937. § 1.3(zzzz), *Algorithmic Trading*. This term means trading in any commodity interest . . . on or subject to the rules of a DCM, where:

(1) One or more computer algorithms or systems determines whether to initiate, modify, or cancel an order, or otherwise makes determinations with respect to an order, including but not limited to: the product to be traded; the venue where the order will be placed; the type of order to be placed; the timing of the order; whether to place the order; the sequencing of the order in relation to other orders; the price of the order; the quantity of the order; the

almost any trading that uses computer programs or software (even merely an Excel spreadsheet) to make a determination with respect to an order—which has become quite commonplace.<sup>13</sup>

Our concern with the Volume Threshold Test is that it doesn't have a nexus to trading by a market participant's proprietary algorithms. Under the Volume Threshold Test, a firm that trades on behalf of many fund clients, regardless of how those orders are transacted (*e.g.*, sent electronically by an FCM) would satisfy the Volume Threshold Test.<sup>14</sup> So, for example, a firm with different business lines that, on average, transacts 19,000 contracts a day in a non-Algorithmic Trading way and 1,000 contracts a day through Algorithmic Trading would be an AT Person, even if the majority of its trading were not conducted through Algorithmic Trading.

We are also concerned that the Supplemental Proposal's AT Person framework is short-sighted and doesn't take into consideration that trading has become, and in the future is likely to only become, increasingly automated. Thus, the definitions are likely to lose meaning as automation becomes the norm and the number of AT Persons expands. We believe the definition of Algorithmic Trading needs to be more precise. Otherwise, all types of market participants that meet the Volume Threshold Test, which, in the future, could be a greater number of market participants, will be subject to Regulation AT. MFA has suggested that one way to address the concerns related to the overly broad definition of algorithmic trading would be to introduce the defined term of "**AT System**" to mean *all computer, network, electronic, technical, automated, or similar systems that directly transmits, receives or processes an AT Order Message*.

## 2. Direct Electronic Access<sup>15</sup>

We are concerned that the definition of Direct Electronic Access ("**DEA**"), like the definition of Algorithmic Trading, is so broad that it is almost meaningless. DEA covers all orders that are electronically submitted, except for orders/modifications/cancellations sent by an FCM which were first received by the FCM from a natural person through oral or written

---

partition of the order into smaller components for submission; the number of orders to be placed; or how to manage the order after submission; and

(2) Such order, modification or order cancellation is electronically submitted for processing on or subject to the rules of a designated contract market; provided, however, that Algorithmic Trading does not include an order, modification, or order cancellation whose every parameter or attribute is manually entered into a front-end system by a natural person, with no further discretion by any computer system or algorithm, prior to its electronic submission for processing on or subject to the rules of a designated contract market.

<sup>13</sup> See MFA March 16, 2016 Letter at p. 11-12.

<sup>14</sup> Separately, we support that the Supplemental Proposal allows a person to voluntarily register as an AT Person. In this way, a market participant could choose to implement its own pre-trade and other controls, rather than be subject to a clearing FCM's controls.

<sup>15</sup> See Supplemental Proposal at 85,391. § 1.3(yyyy), Direct Electronic Access. For purposes of §§ 1.3(x), 1.3(xxxx), 1.80. 1.81. 1.82. 38.255, and 40.20, this term means the electronic transmission of an order for processing on or subject to the rules of a contract market, including the electronic transmission of any modification or cancellation of such order; provided however that this term does not include orders, or modifications or cancellations thereof, electronically transmitted to a designated contract market by a futures commission merchant that such futures commission merchant first received from an unaffiliated natural person by means of oral or written communications.

communications. Due to advancements in technology, only a tiny fraction of all orders to an FCM are received by means of oral or written communications, and this level is likely to further decrease with new developments in technology. We believe that DEA should refer to orders that are transmitted to a DCM without first going through a set of pre-trade risk controls by a registrant subject to Regulation AT.

### 3. AT Order Message<sup>16</sup>

Due to the overly broad definition of Algorithmic Trading, in practice, an AT Order Message would include all of an AT Person's orders, including those from separate businesses which may not be from automated strategies. We believe that only an AT Person's orders from automated strategies should be subject to the AT Person requirements. To the extent an AT Person has other lines of business (*i.e.*, entities under common control with the AT Person), such trading should be subject to the same electronic trading requirements as other market participants. We appreciate that the Supplemental Proposal allows an AT Person to delegate pre-trade and other risk controls,<sup>17</sup> and believe the Commission should clarify in its final rule that an AT Person and an FCM may agree to delegate pre-trade and other risk control responsibilities with respect to only a portion of an AT Person's orders.

### 4. Electronic Trading<sup>18</sup> and Electronic Trading Order Message<sup>19</sup>

We support the definitions of Electronic Trading and Electronic Trading Order Message. We believe, however, that there is little practical difference between these terms and Algorithmic Trading and AT Order Message. As discussed above, we suggest that the Commission provide more precise definitions to give independent meaning to Algorithmic Trading and AT Order Message.

### 5. Algorithmic Trading Source Code<sup>20</sup>

We are concerned with the broad and open-ended nature of the definition of Algorithmic Trading Source Code ("**Source Code**"), which we believe will make compliance with

---

<sup>16</sup> See Supplemental Proposal at 85,391. § 1.3 (www) AT Order Message. This term means each new order submitted through Algorithmic Trading by an AT Person and each modification or cancellation submitted through Algorithmic Trading by an AT Person with respect to such an order.

<sup>17</sup> Supplemental Proposal at 85,392, proposed § 1.80(d).

<sup>18</sup> See Supplemental Proposal at 85,392. § 1.3(dddd) Electronic Trading. For purposes of §§ 1.80, 1.82, 1.83, 38.255, 40.20 and 40.22 of this chapter, this term means trading in any commodity interest as defined in paragraph (yy) of this section on an electronic trading facility as such term is defined by section 1a(16) of the Act, where the order, order modification or order cancellation is electronically submitted for processing on or subject to the rules of a designated contract market.

<sup>19</sup> See Supplemental Proposal at 85,392. § 1.3(bbbbb) Electronic Trading Order Message. This term means each new order submitted by Electronic Trading and each modification or cancellation submitted by Electronic Trading with respect to such an order.

<sup>20</sup> See Supplemental Proposal at 85,392. § 1.3(ccccc) Algorithmic Trading Source Code. Algorithmic Trading Source Code generally means computer commands written in a computer programming language that is readable by natural



recordkeeping requirements unwieldy and so costly that it will put AT Persons at an unfair commercial disadvantage compared to other market participants. For example, as “Algorithmic Trading system” is undefined, we find the term vague as it could refer to the source code of a number of different supporting functions for Algorithmic Trading, such as software for providing system diagnostics or software with respect to a system’s security features. We are also concerned that including “logic embedded in electronic circuits, scripts, parameters input into an Algorithmic Trading system, formulas and configuration files” into the Source Code definition make the definition needlessly broad and would make compliance with preservation requirements extremely burdensome and expensive. For example, a trading server might have hundreds of configuration files, many of which are designed to be ephemeral and not probative, while scripts often include third-party code designed for general use and is accompanied only by generic documentation. Currently, these types of instructions are not documented in the same manner firms typically use for critical trading execution code, and doing so would be an impractical, complex and difficult undertaking. Requiring an AT Person to make records of each aspect of its operating systems will significantly increase regulatory burdens, raise the barriers to entry and deter market participants from becoming AT Persons.

We believe the Commission should adopt an objective standard that can be readily understood and applied by market participants. As proposed in the June 24, 2016 Group Letter, we think the Commission should define Source Code as: a collection of computer instructions as they are originally written (*i.e.*, typed into a computer) in plain text (*i.e.*, human readable alphanumeric characters) comprising executable software capable of exercising discretion over an order on the production environment of a DCM without human intervention.<sup>21</sup> Such discretion includes:

1. The ability to submit, modify, or cancel the order.
2. The ability to determine and set the following order details:
  - Product
  - Price
  - Side
  - Quantity
  - Type of order (*i.e.*, Limit, Market, GTC)
  - When to submit an order affecting request to the DCM
  - Where to submit an order affecting request to the DCM

As discussed at length in the MFA March 16, 2016 Letter and the AIMA 16 March 2016 Letter, we believe Algorithmic Trading should only refer to execution algorithms, which are responsible for sending all order events to the production environment of a DCM, and not investment algorithms, which alone have no effect on a DCM. While we think the most sensible

---

persons. For purposes of §§ 1.81 and 1.84, Algorithmic Trading Source Code shall include at minimum computer code, logic embedded in electronic circuits, scripts, parameters input into an Algorithmic Trading system, formulas, and configuration files.

<sup>21</sup> See June 24, 2016 Group Letter. The Group modeled their source code definition off of the Linux Information Project’s definition of source code: [http://www.linfo.org/source\\_code.html](http://www.linfo.org/source_code.html).

regulatory solution is to focus on controls at market gatekeepers, narrowing the focus from Algorithmic Trading to execution algorithms will permit the Commission to address the principal risks that arise in algorithmic trading, without needlessly diverting regulatory resources to address processes that alone have no impact on the order books of DCMs. Imposing the full battery of controls proposed in Regulation AT to the disparate types of investment models used by market participants will significantly increase compliance costs, but result in little more than a redundant set of controls that address risks which can be adequately covered by pre-trade controls and post-trade surveillance. The risks inherent in algorithmic trading are best addressed by pre-trade controls and effective surveillance without adding an expensive detour into upstream investment processes. This is an area where the driving principles behind Project KISS should apply, where developing a simpler rule that is less burdensome and has less of a drag on the American economy can lead to more effective results for the Commission.<sup>22</sup>

Accordingly, the definition of Source Code for the purposes of Regulation AT should not extend to software used in any other capacities within the market participant or its affiliated companies. It also should not extend to third-party source code to which a market participant lacks access and/or cannot retain due to legal or technical restrictions (*e.g.*, as a licensee or user of software), as further discussed below.

## **B. Pre-Trade & Other Risk Controls**

We have been strong proponents of a two-tier risk control framework, and appreciate that the Commission has incorporated a two-tier risk control framework into the Supplemental Proposal. We have many concerns, however, with the framework in the Supplemental Proposal, including that the regulation continues to be too prescriptive and needs to be more principles and risk-based. The Supplemental Proposal amends § 1.80 on pre-trade risk controls and other controls by incorporating provisions allowing an AT Person to delegate the Regulation AT risk control requirements, and extending the AT Person risk control requirements to an AT Person's Electronic Trading.<sup>23</sup>

Most market participants do not have or use their own proprietary execution algorithm or front-end system to transact their orders. While the Supplemental Proposal recognizes that an AT Person may outsource the execution of its orders and addresses this issue by allowing an AT Person to delegate the pre-trade risk control function to an FCM, we remain concerned with the application of pre-trade risk control requirements on market participants that do not use their own proprietary execution algorithm or front-end system.

First, we do not believe that a market participant/AT Person that uses an investment algorithm to formulate its investment decisions and then sends orders through an FCM's order-entry system for execution on a DCM should be subject to § 1.80. Such a market participant should not be any more responsible for an FCM's compliance with § 1.80 than any other market participant (*i.e.*, a non-AT Person) that manually sends orders through an FCM's order-entry

---

<sup>22</sup> See Giancarlo Boca Remarks, *supra* n. 5.

<sup>23</sup> Supplemental Proposal at 85,392, proposed §§ 1.80(d), (e) and (g).

system for execution on a DCM. The Commission should not treat similarly situated market participants differently. Second, we do not believe it is feasible to require a market participant that delegates the pre-trade risk controls to an FCM to periodically review the FCM's compliance with the § 1.80 requirements. Such market participant may not have the expertise to conduct the necessary due diligence and an FCM is not likely to allow a client to review its proprietary systems. At best, such AT Person would likely receive, on a periodic basis, a certification from an FCM. This requirement would be akin to holding a consumer responsible for whether the driving software and electronics in his or her car and meet the federal safety requirements. We believe the responsibility to comply with § 1.80 requirements should remain solely with the registrant implementing the controls. This change would simplify and reduce the costs associated with Regulation AT.

Accordingly, we recommend that the Commission exclude an AT Person that does not operate a proprietary execution algorithm from the requirements of § 1.80, and to amend § 1.80 so that only the market participant implementing the pre-trade risk and other controls are responsible for compliance with the requirements.

### **C. Development and Testing Requirements for Algorithmic Trading Systems**

As the Commission considers whether to modify requirements regarding the development, monitoring, and compliance of Algorithmic Trading systems under proposed § 1.81,<sup>24</sup> we continue to support the comments and recommendations in the MFA March 16, 2016 Letter with respect to these provisions.<sup>25</sup>

### **D. Maintenance and Commission Access to Source Code**

#### **1. Using the Subpoena Process to Access Source Code**

We remain concerned with the Source Code provisions in the Supplemental Proposal, which include a books and records provision for the maintenance of Source Code and a special call process for the CFTC to access Source Code and related records.<sup>26</sup> We do not object or argue with the CFTC's ability to examine Source Code where appropriate to investigate suspicious market behavior. We are concerned that the Commission is overreaching in its authority to seize intellectual property of registrants and that it has not made the case for why the existing subpoena process is not adequate to serve the Commission's ability to oversee markets. This is also a dangerous regulatory precedent to set and is likely to have a disproportional impact on U.S. businesses in the world economy.

The Commission has emphasized that recordkeeping and Commission access to books and records are central to the Commodity Exchange Act's (the "Act") statutory framework for the

---

<sup>24</sup> See Supplemental Proposal at 85,392, proposed § 1.81; and NPRM at 78,938, proposed § 1.81.

<sup>25</sup> See MFA March 16, 2016 Letter at p. 18-20.

<sup>26</sup> See Supplemental Proposal at 85,393.

oversight of regulated derivatives markets.<sup>27</sup> However, we do not believe that trade secrets and other commercially-valuable intellectual property, including source code, constitutes the books and records which the Act requires registrants to maintain and to provide for prompt access by the Commission and its staff.<sup>28</sup> This position would appear to conflict with other areas of law and practice, such as trade secret law, which puts the onus on owners of intellectual property to protect the confidentiality of such intellectual property. Also, requiring a registrant to provide unfettered access and inspection to its most valuable intellectual property would seem to circumvent and defeat the need and purpose of the subpoena process.

The Commission explains that it is interested in examining Source Code to help it investigate, understand, and respond to significant market disruptions and failures of the price discovery process. We strongly believe that the subpoena process in place would allow the CFTC to fulfill its market oversight responsibilities while providing market participants with a framework that provides greater protection to their intellectual property. The Commission has not shown that the subpoena process is inadequate or that it would not allow the Commission to fulfill its market oversight obligations. The Commission only explains that it would prefer to distinguish the use of subpoenas in investigatory proceedings from access to records by the CFTC Division of Market Oversight (“**DMO Staff**”) in connection with market surveillance.<sup>29</sup> The Commission should not abrogate the property rights of registrants merely for the convenience of the DMO Staff.

We are also concerned with the regulatory precedent the CFTC would set in requiring market participants to allow the government to examine Source Code. In a similar situation, the Associations sent a letter to the China Securities Regulatory Commission (“**CSRC**”) on November 8, 2015 in response to a consultation draft on programme trading. One of the concerns we had was the CSRC’s requirement to access and inspect a market participant’s programme/algorithmic trading.<sup>30</sup> Our members were highly alarmed with this proposal and many were deterred from trading within China. While the CSRC’s proposal and lack of protection for property rights was disappointing, we were very much surprised to find the Commission proposing similar regulation that would subvert a property owner’s due process of law. The national competent authorities of the Member States of the European Union are or will be considering how to oversee algorithmic trading under the Markets in Financial Instruments Directive II. We believe the example the Commission sets with respect to the treatment of intellectual property will play an influential role

---

<sup>27</sup> Supplemental Proposal at 85,347.

<sup>28</sup> *Id.* See also MFA March 16, 2016 Letter at p. 20.

<sup>29</sup> *Id.*

<sup>30</sup> See letter from Jack Inglis, Chief Executive Officer, AIMA, and Richard H. Baker, President and Chief Executive Officer, MFA, to Department of Market Supervision, CSRC, dated Nov. 8, 2015, regarding the Consultation Draft of the Administrative Measures for Programme Trading on Securities and Futures Markets, available at: <https://www.managedfunds.org/wp-content/uploads/2015/11/AIMA-MFA-Comments-to-CSRC-EN-Final-Update-1511081.pdf>.

among international regulators, and one which could ultimately come back to haunt American businesses with valuable intellectual property, as well as other market participants globally.

The Associations fully support the statements by Acting Chair Chris Giancarlo regarding the need to provide property owners with due process of law through the subpoena process before the government can seize their property, and the dangerous regulatory precedent abrogating such rights would create.<sup>31</sup>

## 2. Commission Protections for Source Code

The Supplemental Proposal attempts to provide assurances to market participants with respect to when and how Source Code would be accessed and protected by requiring Commission approval by means of a special call for records and providing that the records are subject to section 8(a) of the Act.<sup>32</sup> Unfortunately, we believe the provisions are far from satisfactory. While Chairman Massad had explained that the CFTC was simply trying to ensure that source code was preserved so that they could look at it if there was a *problem*, we are concerned that under a special call process the Commission and DMO Staff are likely to seek Source Code more frequently than under a subpoena process, especially in light of how regular special calls have become in recent years.<sup>33</sup>

In addition, we are disappointed that the confidentiality provision under proposed § 1.84 does nothing more than restate the existing statutory protections provided to trading strategies, trade secrets and other similar information of market participants. Proposed § 1.84 does not create any new protections, policies or procedures with respect to protecting confidential information, such as trade secrets and other intellectual property. The Commission states that it receives confidential information on a daily basis in a variety of contexts, and it has significant data security measures in place to protect sensitive information from internal or external threats.<sup>34</sup>

Yet despite the Commission's efforts and the regulations in place, we are not confident in the Commission's, nor any other agency's ability to protect confidential information.<sup>35</sup> The list of

---

<sup>31</sup> See Giancarlo Statement of Dissent, *supra* n. 6.

<sup>32</sup> Supplemental Proposal at 85,349.

<sup>33</sup> See, e.g., Response by Timothy Massad, Chairman, CFTC at the Hearing before the House Agriculture Committee and Agriculture Appropriations Subcommittee on the Budget of the Commodity Futures Trading Commission, February 10, 2016 (explaining that the CFTC wants firms to preserve source code, so that if there's a problem, they can reconstruct events).

<sup>34</sup> Supplemental Proposal at 85,348.

<sup>35</sup> See, e.g., CFTC Office of Inspector General ("OIG") Report to Congress, April 1, 2015-September 30, 2015, (raising concerns with the vast majority of servers and network users) available at: [http://www.cftc.gov/idc/groups/public/@aboutcftc/documents/file/oig\\_reporttocongress093015.pdf](http://www.cftc.gov/idc/groups/public/@aboutcftc/documents/file/oig_reporttocongress093015.pdf); and CFTC OIG Assessment of the Most Serious Management Challenges Facing the CFTC, October 26, 2016, (finding that the most serious management challenges for the CFTC are to minimize information security vulnerabilities in its network, and to execute its strategic plan with limited budgetary resources, among others) available at: <http://www.cftc.gov/About/OfficeoftheInspectorGeneral/ssLINK/oigmgmtchall2015>.

federal government cyber breaches is long and growing, including the Central Intelligence Agency (2017), White House (2014), Department of State (2014), Federal Deposit Insurance Corporation (2015, 2016), Federal Aviation Administration (2015), Department of Defense (2015), Internal Revenue Service (2015, 2016), Office of Personnel Management (2015), the Pentagon (2015), the Federal Reserve (2011-2015),<sup>36</sup> Department of Homeland Security and Federal Bureau of Investigation (2016), and Department of Treasury (2016).<sup>37</sup> In October 2015, the CFTC Inspector General issued a report finding that one of the CFTC's most serious management challenges was to minimize information security vulnerabilities in its network.<sup>38</sup> In a 2016 CFTC Inspector General investigation into a potential information technology security incident, the Inspector General found that the CFTC information technology policies and procedures were outdated and not adhered to or applied; employees believed that the computer security training was insufficient; and there was a lack of controls relating to information technology security policies and practices, among other issues.<sup>39</sup>

Government servers are under a constant state of attack—given this new reality and the Commission's unprecedented plan to expand its ability to examine source code as part of market oversight, we believe the Commission must adopt additional regulatory protections for Source Code.

The concerns that market participants have with providing Source Code to the CFTC, include:

- The CFTC will not be able to maintain the confidentiality of Source Code;
- Source Code could be stolen from the CFTC—either electronically or in hard copy;
- Source Code information could be misappropriated; or
- The CFTC could be forced to produce Source Code in relation to a lawsuit or in response to a Member of Congress.

---

<sup>36</sup> See CIA Contractors Likely Source of Latest WikiLeaks Release: U.S. Officials, Reuters, Mar. 9, 2017 available at: <http://www.reuters.com/article/us-cia-wikileaks-idUSKBN16F2AP>; Continued Federal Cyber Breaches in 2015, Riley Walters, Nov. 19, 2015, available at: <http://www.heritage.org/research/reports/2015/11/continued-federal-cyber-breaches-in-2015>. See The IRS Says Identity Thieves Hacked Its Systems Again, Fortune, Feb. 10, 2016, available at: <http://fortune.com/2016/02/10/irs-hack-refunds/>; and Federal Reserve Hacked More than 50 Times in 4 Years, The Huffington Post, June 1, 2016, available at: [http://www.huffingtonpost.com/entry/hackers-breach-federal-reserve-50-times-us\\_574ee0d5e4b0757eae1194c](http://www.huffingtonpost.com/entry/hackers-breach-federal-reserve-50-times-us_574ee0d5e4b0757eae1194c). See also Republican Staff Memorandum to Republican Members, Committee on Science, Space and Technology, July 12, 2016 available at: <https://www.documentcloud.org/documents/2992789-Final-GOP-Interim-Staff-Report-7-12-16.html>.

<sup>37</sup> See Lorenzo Franceschi-Bicchierai, "Hacker Publishes Personal Info of 20,000 FBI Agents," Motherboard, February 8, 2016, available at: <https://motherboard.vice.com/read/hacker-publishes-personal-info-of-20000-fbi-agents>; and News release, "OCC Notifies Congress of Incident Involving Unauthorized Removal of Information," U.S. Department of the Treasury, Office of the Comptroller of the Currency, October 28, 2016, available at: <http://www2.occ.gov/news-issuances/news-releases/2016/nr-occ-2016-138.html>.

<sup>38</sup> Office of Inspector General, CFTC, Assessment of the Most Serious Management Challenges Facing the CFTC, October 26, 2015, available at: <http://www.cftc.gov/About/OfficeoftheInspectorGeneral/ssLINK/oigmgmtchall2015>.

<sup>39</sup> Office of Inspector General, CFTC Investigation into a Potential Information Technology Security Incident, June 27, 2016, available at: [http://www.cftc.gov/idc/groups/public/@aboutcftc/documents/file/oig\\_itsecurity\\_062716.pdf](http://www.cftc.gov/idc/groups/public/@aboutcftc/documents/file/oig_itsecurity_062716.pdf).

In short, the more often that the CFTC has possession of registrant's proprietary Source Code, the greater the likelihood that the information will become compromised, either by hacking or because of the CFTC's failure to guard such information carefully.

We refer the Commission to the MFA March 16, 2016 Letter with respect to enhancing information security protections at the CFTC.<sup>40</sup> We also agree and support Acting Chair Giancarlo's suggestions for steps which the CFTC could take with respect to mitigating concerns relating to the Commission's possession of Source Code by requiring that the CFTC staff: only review Source Code at a market participant's premises or on computers not connected to the Internet; return all Source Code to the property owner once the review is finished; and implement robust internal policies and procedures with respect to reviewing materials related to a market participant's trading strategies, trade secrets and Source Code.<sup>41</sup> Finally, the Supplemental Proposal discusses current statutory and regulatory provisions in place that prohibit an employee from the disclosure of confidential information, including trade secrets.<sup>42</sup> We are concerned that these provisions and the discussion do not cover the prohibition of misappropriation of trade secrets by former employees. To close the gap, we believe the Commission should amend § 140.735-5 to prohibit an employee or former employee from misappropriating confidential information.<sup>43</sup>

We continue to believe that the subpoena process offers market participants greater protection of their proprietary information. We recommend that the Commission consider a preservation requirement with respect to Source Code, not subject to the CFTC's general books and records requirements, as referenced in both the MFA March 16, 2016 Letter and AIMA 16 March 2016 Letter. We further recommend that the Commission balance the rights of property owners with its market oversight responsibilities by using the existing subpoena process for accessing Source Code.<sup>44</sup>

#### **E. Use of Third-Party Algorithmic Trading Systems or Components**

We appreciate that the Commission has tried to address concerns that it received with respect to Regulation AT and market participants that use third-party systems. We are concerned, however, that proposed § 1.85 regarding the use of third-party Algorithmic Trading systems or components is unworkable. The Supplemental Proposal allows AT Persons that use third-party systems to comply with Regulation AT requirements by: (1) obtaining a certification from the third-party that the relevant system or component meets applicable regulatory requirements; (2) obtaining a new certification each time there is a material change to the third-party system; (3) conducting due diligence to reasonably determine the accuracy and sufficiency of a certification

---

<sup>40</sup> MFA March 16, 2016 Letter at 26-27.

<sup>41</sup> See Giancarlo Statement of Dissent, *supra* n. 6.

<sup>42</sup> Supplemental Proposal at 85,349.

<sup>43</sup> Supplemental Proposal at 85,350; 17 C.F.R. § 140.735-5.

<sup>44</sup> MFA March 16, 2016 Letter, at p. 20-27 and AIMA 16 March 2016 Letter at p. 9-12.

provided by a third-party; and (4) remaining responsible for compliance with Regulation AT, including the retention and production of records under § 1.84.<sup>45</sup>

While we believe it is feasible for an AT Person to obtain a certification from an FCM or third-party vendor with respect to Regulation AT requirements, we believe it may be difficult for an AT Person to ensure that it obtains a new certification each time an FCM or third-party vendor makes a material change to its system. This is simply because the AT Person may not be aware of when such changes are made.

The Supplemental Proposal explains that “the due diligence required to be performed by the AT Person under Supplemental proposed § 1.85(c) is limited to the accuracy of the certification” and that “detailed technical audits are not required”.<sup>46</sup> It is not clear to us how an AT Person would be able to ensure the accuracy of a certification without verifying compliance through a technical audit. We are concerned that the due diligence requirement of AT Persons with respect to third-parties would be unfeasible and overly burdensome. Similarly, we are concerned that the Supplemental Proposal imposes liability on an AT Person for a third-party’s compliance with Regulation AT, including the maintenance and production of records, such as Source Code. We believe in these circumstances it is unfair to hold a market participant liable for compliance over systems which it lacks access, whether due to legal or technical restrictions – imagine holding a smart phone user responsible for the phone’s operating system software glitches.

The cost and liability concerns with proposed § 1.85 requirements are so great that AT Persons may avoid using third-party vendors or small start-up firms for services to connect to a DCM. Rather than discourage innovation and new technology, the Commission, like the Securities and Exchange Commission, should further consider how the regulatory environment can most effectively address these new technologies and promote safer and more efficient markets.<sup>47</sup> In this respect, we strongly support Acting Chair Giancarlo’s forward leaning “Embracing FinTech” initiative and urge the CFTC to be a leader in adopting the “do no harm” approach to financial technology.<sup>48</sup>

We recommend that the Commission schedule roundtables and/or meet with financial technology companies to further explore solutions with respect to regulation and new technology. We also recommend that the Commission eliminate requirements to hold AT Persons liable for a third-party’s Algorithmic Trading system or compliance with Regulation AT.

\* \* \* \* \*

---

<sup>45</sup> See Supplemental Proposal at 85,393. §1.85, Use of third-party Algorithmic Trading systems or components.

<sup>46</sup> See Supplemental Proposal at 85,352.

<sup>47</sup> See SEC to Hold Forum to Discuss Fintech Innovation in the Financial Services Industry, September 27, 2016, available at: <https://www.sec.gov/news/pressrelease/2016-195.html>.

<sup>48</sup> See Giancarlo Boca Remarks, *supra* n. 5.



Mr. Kirkpatrick  
May 1, 2017  
Page 17 of 17

The Associations appreciate the opportunity to provide comments and recommendations on Regulation AT. We would welcome the opportunity to discuss our views on Regulation AT with the Commission or its staff in greater detail. If the staff has any questions, please do not hesitate to contact Jennifer Han, Associate General Counsel, MFA, at (202) 730-2600, or Oliver Robinson, Associate Director, AIMA, at (+44) 2078228380.

Respectfully Submitted,

/s/ Stuart J. Kaswell

Stuart J. Kaswell  
Executive Vice President & Managing Director  
General Counsel  
Managed Funds Association

/s/ Jiří Król

Jiří Król  
Deputy CEO, Global Head  
of Government Affairs  
Alternative Investment Management  
Association

CC: The Honorable Chris Giancarlo, Acting Chair  
The Honorable Sharon Bowen, Commissioner  
Amir Zaidi, Director, Division of Market Oversight  
Sebastian Pujol Schott, Associate Director, Division of Market Oversight

## APPENDIX A

March 16, 2016

### **Via Website Submission**

Christopher Kirkpatrick  
Secretary of the Commission  
Commodity Futures Trading Commission  
Three Lafayette Centre  
1155 21<sup>st</sup> Street, NW  
Washington, DC 20581

**Re: RIN 3038-AD52; Proposed Regulation Automated Trading**

Dear Mr. Kirkpatrick:

Managed Funds Association<sup>1</sup> (“**MFA**”) appreciates the opportunity to submit comments to the Commodity Futures Trading Commission (the “**CFTC**” or the “**Commission**”) on its notice of proposed rulemaking on Regulation AT (“**Regulation AT**”).<sup>2</sup> MFA supports the Commission’s goal of modernizing regulatory oversight of automated trading with risk controls, transparency measures, and other safeguards with respect to U.S. designated contract markets (“**DCMs**”). The Commission has been thoughtful in proposing Regulation AT and the Proposing Release provides many regulatory considerations and examples of market practice for public comment.

We are concerned, however, that Regulation AT attempts to address too many separate regulatory issues under a single umbrella—each of which deserves and requires greater study and public comment. We believe that Regulation AT should be broken into five major categories/objectives, including: (1) a registration regime to capture previously unregistered market participants; (2) marketplace risk controls; (3) standards for the development, testing, reporting, and retention of trading software; (4) a self-trade prevention framework; and (5) a public

---

<sup>1</sup>Managed Funds Association (“**MFA**”) represents the global alternative investment industry and its investors by advocating for sound industry practices and public policies that foster efficient, transparent, and fair capital markets. MFA, based in Washington, DC, is an advocacy, education, and communications organization established to enable hedge fund and managed futures firms in the alternative investment industry to participate in public policy discourse, share best practices and learn from peers, and communicate the industry’s contributions to the global economy. MFA members help pension plans, university endowments, charitable organizations, qualified individuals and other institutional investors to diversify their investments, manage risk, and generate attractive returns. MFA has cultivated a global membership and actively engages with regulators and policy makers in Asia, Europe, North and South America, and many other regions where MFA members are market participants.

<sup>2</sup>80 *Fed. Reg.* 78,824 (Dec. 17, 2015) (hereinafter the “**Proposing Release**”).

disclosure framework with respect to market making and trading incentive programs. In our view, Regulation AT is overly expansive in breadth and scope, and uses an unduly broad brush to regulate automated trading by disparate types of market participants. We appreciate the issues Regulation AT tries to address, but believe there are more targeted and cost-effective ways to address the Commission's concerns.

MFA members generally find that the current exchange-traded derivatives markets function well. The U.S. futures markets, as efficient, low cost, and liquid markets, are an essential tool for our Nation's economy. These markets allow MFA's members to invest and manage risk in the funds they manage for their investors. Unfortunately, as proposed, Regulation AT has the potential to significantly increase the cost of using the futures markets while diminishing the liquidity profile of these markets. Accordingly, we ask the Commission to consider the comments below outlining the drawback that we believe the proposal would entail. As discussed below, we believe that there are other, less intrusive approaches that will achieve the Commission's goals.

## I. EXECUTIVE SUMMARY

MFA respectfully urges the Commission to consider addressing each of the five categorical areas under Regulation AT in separate stages and as necessary. We have carefully reviewed and considered Regulation AT and the underlying data supporting the proposals. We are concerned, however, that despite the numerous new and prescriptive risk requirements, the Regulation AT framework would not provide for safer, more efficient or effective futures marketplaces. In fact, we are concerned that it would create new risks, impose greater regulatory burdens, and substantially raise costs, putting the U.S. futures markets out-of-reach for many U.S. and foreign end-users looking to hedge or manage risk. In this letter, we provide a number of recommendations and comments, including:

- **Adopt Centralized Marketplace Risk Controls** – MFA recommends that in lieu of adopting Regulation AT as proposed, the Commission adopt regulation requiring centralized pre-trade risk controls at designated contract markets (“DCMs”) and clearing member futures commission merchants (“clearing FCMs”). We believe that such controls at the DCM and clearing FCM-levels would be highly effective in preventing marketplace disruptions. This approach would share responsibilities along functional lines. In addition, we believe that the Commission should address other derivatives marketplace concerns identified in Regulation AT through separate rulemakings and in different stages.
- **Adopt a More Flexible Framework rather than a One-Size-Fits-All Approach** – MFA is concerned that Regulation AT has a one-size-fits-all framework, which singularly regulates all market participants that use any automation in trading without taking into consideration the type of automation or the different category, business, or operational size of the market participant.
  - MFA recommends that the Commission narrow the focus and scope of Regulation AT to exclude commodity trading advisors (“CTAs”) and commodity pool operators (“CPOs”). Instead, to address concerns relating to CTAs/CPOs, MFA recommends that the Commission direct the National Futures Association (“NFA”)

to promulgate CTA/CPO regulatory requirements on operational systems risk controls; and to report to the Commission on data that it collects from an amended CTA/CPO Self-Examination Questionnaire that includes questions on operational systems risk controls. If necessary, the Commission should amend its Part 4 regulations to address CTA/CPO operational systems risk concerns related to algorithmic trading in a manner suitable for CTA and CPO businesses and operations.

- To the extent that the Commission determines to proceed with a broad Regulation AT framework that applies to all categories and sizes of market participants and different types of algorithmic trading functions, MFA believes that the Commission needs to adopt a more flexible framework. The Commission should identify specific marketplace concerns with respect to algorithmic trading activities and require market participants to prevent marketplace disruptions by: (1) using execution systems with pre-trade risk controls (when and if using algorithmic execution systems); (2) adopting development and testing standards reasonably designed to prevent operational systems risks and marketplace disruptions; (3) retaining source code; and (4) adopting monitoring, compliance and training programs reasonably designed to prevent operational systems risks and marketplace disruptions.<sup>3</sup>
- **Adopt a Source Code Retention Requirement** – MFA has strong concerns with Regulation AT’s source code repository requirement and recommends that the Commission replace it with a source code retention requirement.
- **Retain the Current Self-Trade Surveillance System** – MFA believes that the current DCM rules regarding self-trading are effective, and that the data does not justify the creation of an entirely new federal regulatory regime on self-trading.
- **Require Greater Disclosures with respect to Market Making and Trading Incentive Programs** – MFA supports regulation requiring DCM disclosures and surveillance of market making and trading incentive programs.

## II. CFTC SHOULD ADOPT TARGETED REGULATORY SOLUTIONS TO ADDRESS MARKETPLACE RISK

Like many components of the global financial markets, the U.S. derivatives markets have evolved significantly in recent years, due to CFTC regulation that has fostered an environment that has allowed innovation to flourish, and the rapid pace of technological advances and industry innovation. As the CFTC recognizes, the derivatives markets have transitioned from

---

<sup>3</sup> See, e.g., 17 C.F.R. § 275.206(4)-7; Investment Advisers Act Rule 206(4)-7, Compliance procedures and practices (directing investment advisers to “adopt and implement written policies and procedures reasonably designed to prevent violation, by you and your supervised persons, of the Act and the rules that the Commission has adopted under the Act”). We believe the Commission could take a similar approach with respect to algorithmic trading and marketplace risk.

manual processes to highly automated trading and trade matching systems.<sup>4</sup> End-users and investors, such as CTAs and CPOs, similarly have developed and modernized their trading and investment programs to remain competitive in an increasingly efficient market and to ensure that their systems and processes remain compatible with the trading systems employed by introducing brokers, floor brokers, FCMs, swap dealers, swap execution facilities, and DCMs. In fact, today's CPOs and CTAs simply *must* use software and electronic trading platforms in order to achieve best execution. Many MFA members, for example, operate signal-driven or algorithmic trading strategies that can operate at a range of speeds and generally within real-time human intervention; at the same time, even MFA members that are fundamental futures and equities managers are utilizing algorithms to data-mine for new sources of alpha, back-test theories, execute trades, and manage risk.<sup>5</sup>

Investing and trading in the 21<sup>st</sup> century continues to evolve as investors/traders of all stripes use automated tools to enhance their hedging and risk management activity. MFA supports the Commission's initiative of modernizing its regulatory framework to take into consideration the automated and algorithmic trading environment. Regulation, however, should be tailored to address the concerns that the Commission has identified, and should be proportionate and scalable, in order to be cost-effective and manageable for both regulators and market participants.<sup>6</sup> Overly prescriptive and extraneous regulations will not only stunt innovation and growth but hamper the ability of market participants to continue using the futures markets for the very purposes for which they were created—*i.e.*, hedging and risk management.

#### **A. *Risk Controls Should Be Centralized***

MFA is concerned that the Regulation AT framework is overly broad and elaborate, which would make implementation expensive and burdensome for market participants and regulators. Regulation AT, as proposed, would regulate - *in the same manner* - virtually any market participant that uses any automation with respect to trading, without taking into consideration the type of automation or the different category, business or operational size of the market participant. Based on the Commission's own cost-benefit and regulatory flexibility analyses, we believe this is not the Commission's intent.

Recognizing that all market participants, regardless of registration status or type of trader, have the potential to cause marketplace disruptions, we believe the single most effective way to prevent marketplace risk is through centralized risk controls at the DCM. Futures exchanges offer market participants a myriad of ways to access and trade on their marketplaces. We do not believe it would be efficient or cost-effective to apply the full panoply of Regulation

---

<sup>4</sup>*Id.* at 78,825.

<sup>5</sup> As the Commission knows, some trading entities operate true high-frequency strategies. While that portion of the market does overlap with the trading strategies of some MFA members, this comment letter in general will not address the special needs and concerns of those market participants.

<sup>6</sup>*See* Section 15(a) of the Commodity Exchange Act, Consideration of Costs and Benefits.

AT requirements to the majority of futures market participants.<sup>7</sup> Rather, we believe that risk controls, such as those proposed in § 1.80 should be applied at the DCM-level and clearing FCM-level. Requiring standardized risk controls at the DCM and clearing FCM-levels would ensure that all market participant orders go through the same set of controls—whether orders from a market maker or an end-user using manual processes to invest or hedge risk.

Moreover, the general infrastructure for addressing marketplace risk through a centralized approach already exists. DCMs/derivatives clearing organizations provide clearing FCMs with pre-trade risk controls and real-time tools to manage risk with respect to their clients. For example, the CME Group provides clearing FCMs with the ability to set controls and calculate positions for each client, including:

- Long and Short exposure limits;
- Maximum Buy/Sell quantity limits;
- Real-time open and filled position calculations;
- Margin rate;
- Real-time credit control alerts and notifications;
- Order blocking;
- Order cancellation;
- Kill switch.<sup>8</sup>

The CME Group also offers additional risk management tools, such as order cancellations upon involuntary disconnection. Currently, all CTAs and CPOs use clearing FCMs; which conduct due diligence on their clients and impose stringent risk controls set at customized levels. Given that a centralized framework for addressing marketplace risk already exists, we believe that the starting point should be for the Commission to review and build upon the existing infrastructure, rather than to require a significant portion of market participants to each build the same risk infrastructure on their own systems.<sup>9</sup> While a multi-layered approach to pre-trade risk controls is beneficial; requiring multiple layers (DCM, clearing FCM, FCM, and market participant) to implement the *same* risk controls would be ineffective and an inefficient use of

---

<sup>7</sup> See *infra* Sections IV.A.1 and 2 explaining that Regulation AT, as proposed, would capture a broad swath of market participants.

<sup>8</sup> See CME Globex Credit Controls, available at: [http://www.cmegroup.com/tools-information/webhelp/globex-credit-controls/Content/CME\\_Globex\\_Credit\\_Controls\\_Management.html](http://www.cmegroup.com/tools-information/webhelp/globex-credit-controls/Content/CME_Globex_Credit_Controls_Management.html). See also, ICE Tips, Clearing and Bilateral Credit Management, February 20, 2009, available at: <https://www.theice.com/publicdocs/ChemConnectCreditTip.pdf>.

<sup>9</sup> We understand that DCMs offer and FCMs already implement the pre-trade risk controls in proposed § 1.80. See *supra* Section IV.B.

resources. To achieve an effective multi-layered strategy for addressing trading risk, beyond centralized risk controls, individual market participants should customize risk controls to their strategies—which CTAs and CPOs already do as fiduciaries to their clients/investors.

The Commission should assess and evaluate through a data-driven process whether additional risk controls should be implemented by DCMs; and whether clearing FCMs are effectively implementing existing pre-trade risk controls and setting appropriate limits for their clients, prior to determining whether more needs to be done. We believe that the standardized controls at the DCM and clearing FCM-levels create a robust framework for addressing marketplace risk. While we believe all market participants using trading algorithms—whether proprietary algorithms or third party vendor algorithms— should have appropriate risk controls in place, we believe it is most effective to allow market participants to customize their risk controls to their individual trading activities. Similarly, we believe a more effective risk control measure would be to require market participants to develop their own internal policies and procedures, including development, testing, monitoring and compliance protocols, tailored to their strategies, rather than to prescribe industry procedures, which may be ill-suited to individual strategies.<sup>10</sup>

Finally, a major advantage of requiring centralized risk controls is that it would be more transparent and easier for regulators, such as the Commission, to oversee and enforce. Regulation AT, on the other hand, would require DCMs to expend considerable resources overseeing the risk controls of hundreds, if not thousands, of market participants and clearing FCMs. Moreover, in this respect, we believe Regulation AT is flawed if the expectation is that DCMs would be able to assess an “AT Person’s” or clearing member FCM’s compliance with Regulation AT based on compliance reports.

Accordingly, MFA recommends that in lieu of adopting Regulation AT as proposed, the Commission should adopt regulation requiring centralized pre-trade risk controls at DCMs and clearing FCMs. We believe such controls at the DCM and clearing FCM-levels would be highly effective in preventing marketplace disruptions at a fraction of the cost of Regulation AT.

### ***B. The Commission Should Address Other Marketplace Changes in Stages***

Regulation AT introduces several different regulatory objectives, which, in addition to marketplace risk controls, include a registration regime to capture previously unregistered market participants; standards for the development, testing, reporting, and retention of trading software; a self-trade prevention framework; and a disclosure framework with respect to market making and trading incentive programs. The Commission has raised a host of important issues, which we believe the Commission should address through targeted proposals in separate stages. By combining several significant market issues together, we are concerned that each proposal will not receive the full attention that each deserves by the public and the Commission. We would like to see the Commission and market participants develop data-driven solutions to

---

<sup>10</sup> See *supra* n. 3.

address each issue in a thoughtful and data-driven manner.<sup>11</sup> The Commission should host separate roundtables on each issue.

In addition, we are concerned that requiring the industry to implement multiple major regulatory changes at once will introduce another level of market risk by requiring market participants to spread their resources too thinly. Accordingly, MFA recommends that the Commission consider and address each of the major regulatory issues mentioned above through separate rulemakings and in different stages.

### **III. GENERAL COMMENTS ON REGULATION AT REGARDING CTAS AND CPOS**

#### ***A. Algorithmic Trading Regulation Should Not Be One-Size-Fits-All***

We believe Regulation AT's one-size-fits-all approach is highly problematic in practice, especially as "algorithmic trading," as defined in the Proposing Release, can be read to capture nearly any trading that involves automation. Regulation AT establishes a broad framework that attempts to singularly regulate very disparate categories and types of market participants and their activities. We are strongly concerned that Regulation AT does not make adequate distinctions between different types of market participants, nor does it recognize the different business structures, business models and operational sizes of market participants. While Regulation AT's approach may be appropriate for entities with large operations, such as DCMs, FCMs, clearing member FCMs, and Swap Dealers, it is not appropriately drafted for CTAs and CPOs.

CTAs and CPOs are institutional investors/financial end-users. The level of investor assets that they manage may vary, but generally their operations are significantly smaller than DCMs and FCMs. CTAs and CPOs engaged in algorithmic trading strategies already have risk controls and other processes in place. We believe that Regulation AT would be very burdensome for CTAs and CPOs because it prescribes measures which are not appropriately tailored for the business or strategies of CTAs/CPOs.<sup>12</sup> We believe that the compliance costs associated with Regulation AT would likely create barriers to entry for new participants, harm competition and limit investor choice. We also are concerned that Regulation AT would have a disproportionate impact on CTAs and CPOs, would discourage use of exchange-traded derivatives markets, and would lead to decreased liquidity in the futures markets.

Beyond the significant compliance costs associated with Regulation AT for CTAs and CPOs, we simply do not believe the one-size-fits-all framework appropriately or effectively addresses marketplace risk relating to algorithmic trading by CTAs and CPOs. As discussed further below in section IV.B, we believe that pre-trade risk controls would not be particularly

---

<sup>11</sup> MFA urges the Commission to re-propose the various portions of the proposal to solicit more extensive comment on these various subjects. MFA is concerned that the Commission will not receive sufficiently detailed comments on the current multifarious release.

<sup>12</sup> As discussed further in Section V on cost estimates, we believe the costs associated with Regulation AT for CTAs and CPOs are significantly greater than estimated by the Commission.



relevant or meaningful with respect to CTAs' or CPOs' investment algorithms.<sup>13</sup> Further, we are concerned that Regulation AT's development, testing and recordkeeping requirements with respect to algorithmic trading systems are not proportionate or scalable.

***B. Use the Existing Regulatory Framework to Oversee CTAs and CPOs***

After standardized risk controls at DCMs, we believe that operational risks associated with automated trading, which the Commission cites as the rationale for Regulation AT, would be best addressed through regulatory interpretive guidance and best practices. For example, recently the National Futures Association ("NFA") issued guidance under existing rules with respect to information systems security programs,<sup>14</sup> and added a new cybersecurity section to the NFA Self-Examination Questionnaire.<sup>15</sup> NFA explained in its interpretive notice that:

NFA recognizes that, given the differences in the type, size and complexity of operations of Members' businesses including but not limited to their customers and counterparties, markets and products traded, and the access provided to trading venues and other industry participants, Members must have an appropriate degree of flexibility to determine how best to diligently supervise information security risks. Accordingly, this Interpretive Notice is designed to establish 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. Given the rapidly changing nature of technology and threats to information systems, NFA's policy is not to establish specific technology requirements.<sup>16</sup>

We believe that the nature of operational systems risks is similar to information systems security risks in that the risks are derived from the unique and specific systems of market participants. In this sense, we encourage the Commission to address operational systems risks related to algorithmic trading in the same manner.

MFA members are regulated quite broadly by the CFTC both in terms of their conduct under the Commission's rules that govern all market participants, as well as under specific rules for registered entities as CTAs and CPOs. In fact, only in the past few years have a large number of CPOs become subject to expanded Commission oversight. First, in 2012, the

---

<sup>13</sup> An investment algorithm is investment software that analyzes data to decide which contracts to buy or sell. For example, an investor with European investments may develop software that incorporates proprietary mathematical formulas, for determining whether and how many Euro FX futures contracts to purchase in order to hedge investment risk from changes in the exchange rate.

<sup>14</sup> See NFA Compliance Rules 2-9, 2-36 and 2-49: Information Systems Security Programs (effective March 1, 2016), available at: <http://www.nfa.futures.org/nfamanual/NFAManual.aspx?RuleID=9070&Section=9%20>.

<sup>15</sup> See, e.g., NFA Notice I-16-10 (Feb. 29, 2016), available at: <http://www.nfa.futures.org/news/newsNotice.asp?ArticleID=4701>.

<sup>16</sup> See *supra* n.8.

Commission eliminated an exemption from CPO registration,<sup>17</sup> which in combination with the Commission's new statutory oversight authority over swaps,<sup>18</sup> resulted in a significant number of Securities and Exchange Commission ("SEC") registered investment advisers becoming dual registrants. Preparing for registration was not a small undertaking, as firms had to: review and revamp their compliance programs to comply with the CFTC's Part 4 regulations; become NFA members and comply with NFA bylaws, rules and requirements; and register principals and associated persons with NFA and have staff pass proficiency requirements (*e.g.*, Series 31 exam); among other requirements. While many of the SEC and CFTC requirements for advisers and CPOs are similar, they are not identical and required members to expend a substantial commitment of time and resources in order to comply (including the request for multiple CFTC staff no-action and or exemptive relief letters). Dually registered firms now face multiple exams and regulatory inquiries from the SEC Office of Compliance Inspections and Examinations, NFA, and other self-regulatory organizations, such as the Financial Industry Regulatory Authority, CBOE, CME and ICE, depending on the range of types of securities and derivatives they employ.

Secondly, in 2012, the CFTC adopted a significant new requirement for CTAs and CPOs to prepare and file lengthy analyses of the managed accounts they advise or the commodity pools they operate, (Form CTA-PR and Form CPO-PQR) in order to provide the Commission with information to help with analyses regarding systemic risk.<sup>19</sup> These reports can run up to 150 pages and require thousands of hours per year to produce.

Given the extensive new regulatory regime and reporting requirements for CTAs/CPOs, it seems unreasonable to impose another, separate system of recordkeeping, reports and requirements without first considering whether the existing framework provides sufficient oversight. To the extent that the Commission believes it needs more information from CTAs or CPOs or that these registered entities need enhanced controls, we would strongly urge the Commission to direct the NFA to issue rules addressing operational systems risks related to algorithmic trading and to amend its Self-Examination Questionnaire. From the data the NFA collects through its Self-Examination Questionnaire, the Commission would be able to assess whether additional requirements are necessary to address risk concerns. If, after thorough review, the Commission determines that additional controls and documentation requirements are in fact needed, we believe the Commission should use the existing regulatory framework and amend its Part 4 regulations to address CTA/CPO operational systems risk concerns related to algorithmic trading in a manner suited for CTA and CPO businesses and operations. We think that such a targeted approach would more precisely achieve the Commission's goals at lower cost.

Accordingly, we recommend that the Commission narrow the focus and scope of Regulation AT to exclude CTAs and CPOs; and to direct NFA to promulgate CTA/CPO regulatory requirements on operational systems risk controls related to algorithmic trading and to report to the Commission on data that it collects from an amended CTA/CPO Self-Examination

---

<sup>17</sup> Commodity Pool Operators and Commodity Trading Advisors: Compliance Obligations, 77 *Fed.Reg.* 11,252 (Feb. 24, 2012), available at: <http://www.cftc.gov/idc/groups/public/@lrfederalregister/documents/file/2012-3390a.pdf>.

<sup>18</sup> The Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. 111-203.

<sup>19</sup> *See supra* n. 16.

Questionnaire that includes questions on operational systems risk controls. Once the Commission has more information regarding CTA/CPO operational systems risk controls related to algorithmic trading, it will be in a better position to determine whether and how to amend the CFTC Part 4 regulations.

#### **IV. SPECIFIC COMMENTS ON REGULATION AT**

*First*, as discussed above, MFA recommends that in lieu of adopting Regulation AT as proposed, the Commission adopt regulation requiring centralized pre-trade risk controls at DCMs and clearing FCMs. We believe centralized controls at the DCM and clearing FCM-levels would be highly effective in preventing marketplace disruptions. In addition, we believe the Commission should address other derivatives marketplace concerns identified in Regulation AT through separate rulemakings and in different stages.

*Second*, to the extent the Commission determines to adopt Regulation AT, MFA recommends that the Commission exclude CTAs and CPOs from Regulation AT. Instead, to address concerns relating to CTAs/CPOs, MFA recommends that the Commission direct NFA to promulgate CTA/CPO regulatory requirements on operational systems risk controls; and to report to the Commission on data that it collects from an amended CTA/CPO Self-Examination Questionnaire that includes questions on operational systems risk controls. If necessary, the Commission should amend its Part 4 regulations to address CTA/CPO operational systems risk concerns related to algorithmic trading in a manner suitable for CTA and CPO businesses and operations.

MFA has strong concerns with Regulation AT, as proposed, and believes that its approach to addressing operational systems risks related to algorithmic trading is flawed. We are concerned by the prescriptive, detailed and burdensome nature of Regulation AT's requirements, which we do not believe would make the derivatives markets safer or less prone to market disruptions. MFA believes that the Commission should not adopt Regulation AT. Nevertheless, in the event the Commission declines to accept our recommendations, we have identified specific concerns and provide comments on Regulation AT below.

##### **A. Regulation AT Definitions**

###### **1. Algorithmic Trading<sup>20</sup>**

The terms “automated trading” and “algorithmic trading” have become catchall terms for any trading that uses computer programs or software. As proposed, the term

---

<sup>20</sup>See Proposing Release at 78,937. § 1.3(zzzz), *Algorithmic Trading*. This term means trading in any commodity interest . . . on or subject to the rules of a DCM, where:

(1) One or more computer algorithms or systems determines whether to initiate, modify, or cancel an order, or otherwise makes determinations with respect to an order, including but not limited to: the product to be traded; the venue where the order will be placed; the type of order to be placed; the timing of the order; whether to place the order; the sequencing of the order in relation to other orders; the price of the order; the quantity of the order; the

“Algorithmic Trading” would capture any trading where a computer system was used to make a determination with respect to an order, and would only exclude orders manually entered into a front-end system by a natural person. We are concerned that the definition of Algorithmic Trading is overly broad as it doesn’t distinguish between different types of automated functions, and would capture a majority of registered market participants.

Not all algorithmic trading is the same. Generally, algorithmic trading can be divided into two categories: (1) execution algorithms, which determine the most efficient method of buying or selling a contract and then initiate the purchase or sale orders; and (2) investment algorithms, which are trading or investment software that analyze data to decide which contracts to buy or sell. For example, a CPO may determine through its proprietary investment algorithm that it wants to buy 200 Euro FX futures contracts, it might then use a third party execution algorithm to determine the most cost-efficient way to buy 200 contracts and deploy orders. These differences are significant and should not be treated in the same manner under Regulation AT.

While the Algorithmic Trading definition attempts to exclude trading that is manually executed, we believe it would capture trading by many market participants, including those that use manual processes to determine their investment or hedging strategies. The financial industry, like every other industry sector, has modernized and automated its processes, and utilizes electronic tools in trading and investing. Most commonly, market participants—whether they use manual processes or software tools to determine their orders—access a DCM through an independent software vendor (“ISV”) (typically, provided by their clearing FCM or by the DCM) that provides front-end connection and automated execution software and/or related services.<sup>21</sup> Such software may include features that automate the order-entry process by allowing a market participant to click-and-drag data, such as from a spreadsheet or other document. An ISV may also offer generic trading algorithms such as Volume Weighted Average Price (“VWAP”) engines or reserve quantity orders (*i.e.*, iceberg orders), or other algorithmic trading tools, which are developed, monitored, and tested by the ISV. Thus, *fewer and fewer* market participants are manually entering orders into a front-end system and trading without the use of trading software.

We believe the term Algorithmic Trading is overly broad and generic; and not particularly meaningful. Our concern with such a broad definition is that many market participants would become subject to Regulation AT as AT Persons; and that Regulation AT would regulate all algorithmic trading functions in the same manner (like applying a specific requirement to both apples and oranges). Should the Commission adopt standardized requirements across all trading

---

partition of the order into smaller components for submission; the number of orders to be placed; or how to manage the order after submission; and

(2) Such order, modification or order cancellation is electronically submitted for processing on or subject to the rules of a designated contract market; provided, however, that Algorithmic Trading does not include an order, modification, or order cancellation whose every parameter or attribute is manually entered into a front-end system by a natural person, with no further discretion by any computer system or algorithm, prior to its electronic submission for processing on or subject to the rules of a designated contract market.

<sup>21</sup> See, *e.g.*, a list of Independent Software Vendors, available at: <https://www.theice.com/connectivity/isv>.

algorithm types and functions, as Regulation AT attempts to do, the regulatory requirements would need to be much *more general* in order to be applicable and appropriate for all trading algorithms.

Another way to address the concerns related to an overly broad definition of algorithmic trading would be to introduce the defined term of “**AT System**” to mean *all computer, network, electronic, technical, automated, or similar systems that transmits, receives or processes an AT Order Message*. The advantage of limiting the Regulation AT requirements to an AT System is that it would exclude other automated systems of an AT Person, such an email system that received messages relating to an order.

## 2. AT Person<sup>22</sup>

Our concern with the AT Person concept is that it lumps disparate categories of market participants and trading activities together and subjects them to the same prescriptive requirements. Regardless of whether a registered CTA/CPO uses an execution algorithm, a third-party execution algorithm, or an investment algorithm, it would be similarly subject to Regulation AT.<sup>23</sup>

One way for the Commission to narrow the scope of AT Person would be to define it as *a registrant that engages in Algorithmic Trading through an AT System that it developed and operates*. This would narrow the scope of Regulation AT to execution algorithms, rather than all algorithms. A market participant that uses an investment algorithm, by necessity, uses an execution algorithm—either proprietary or third party—to send orders to a DCM. Execution algorithms directly interface with the market, and in general, share the same objective of efficient execution. As such, it would be easier to standardize regulatory controls with respect to these algorithms. Investment algorithms, on the other hand, can have diverse and disparate objectives and functionalities, making customized controls a necessity.<sup>24</sup>

An additional benefit to redefining AT Person as a registrant that engages in Algorithmic Trading through an AT System that it developed is that it would exclude persons using software developed, provided and/or maintained by a third party to route orders and trade (*i.e.*, a third party execution algorithm). Many market participants use a third party’s, ISV’s, or even a DCM’s execution algorithm to submit orders to a DCM marketplace. We believe it would be unfeasible for such market participants to comply with Regulation AT with respect to a third party’s execution algorithm. We also do not believe it would be a cost-effective framework for

---

<sup>22</sup>See Proposing Release at 78,937. § 1.3(xxxx), *AT Person*. This term means any person registered or required to be registered as a—

(1) Futures commission merchant, floor broker, swap dealer, major swap participant, commodity pool operator, commodity trading advisor, or introducing broker that engages in Algorithmic Trading on or subject to the rules of a designated contract market; or

(2) Floor trader.

<sup>23</sup> A commodity pool or a managed account should not be considered to be an AT Person. If such entities were to be considered AT Persons, there could be tens of thousands of AT Persons.

<sup>24</sup> See *infra* section IV.C and D for more discussion.

the CFTC to subject thousands of market participants to Regulation AT, which we believe, as drafted, is burdensome and likely to deter market participants from using the U.S. futures markets to hedge or manage risk.

3. Algorithmic Trading Compliance Issue<sup>25</sup>

The Proposing Release notes that the term “Algorithmic Trading Compliance Issue” is analogous to the SEC’s Regulation Systems Compliance and Integrity (“**Reg SCI**”)<sup>26</sup> definition of “Systems compliance issue.”<sup>27</sup> However, we do not believe that an analogous definition is appropriate. The SEC designed a cost-effective framework to oversee automated systems by focusing on critical infrastructure, rather than broadly on market participants as Regulation AT. We believe it would make more sense for Algorithmic Trading Compliance Issue to be analogous to Systems Compliance Issue if Regulation AT were to share a more analogous framework as Reg SCI, with centralized regulatory controls.

In addition, Reg SCI generally applies to self-regulatory organizations that are stringently regulated and must submit rules to the SEC for approval before adoption. While the registrant categories under AT Person are highly regulated by the Commission, they are not self-regulatory organizations and their rules/requirements are not subject to Commission public notice and comment and Commission approval prior to adoption. In this respect, we are strongly concerned that the “AT Person’s own internal requirements, or the requirements of the AT Person’s clearing member” are too general and broad.

A market participant generally establishes internal policies and procedures or “internal requirements” for all aspects of its business as prudent business practice and to prevent the market participant from violating statutory or regulatory requirements. A firm may often set high internal standards, above and beyond legal and regulatory requirements. However, if an AT Person could be held liable for not meeting all its own internal requirements, then very quickly AT Persons would change their internal requirements to the minimum requirements by law or regulation or to be more general than they otherwise might be to ensure that they never violate internal requirements. Regulation should promote high industry standards, and threatening firms with regulatory sanctions for failure to adhere to self-imposed standards disincentivizes behavior that should be encouraged. We believe this is contrary to the Commission’s objective of promoting high standards in risk controls and operations; and, thus, believe the definition of Algorithmic Trading Compliance Issue would need to be more specific and refer to an AT Person’s requirements under §§ 1.81 and 1.83.

---

<sup>25</sup>See Proposing Release at 78,937. § 1.3(tttt), *Algorithmic Trading Compliance Issue*. This term means an event at an AT Person that has caused any Algorithmic Trading of such entity to operate in a manner that does not comply with the Commodity Exchange Act or the rules and regulations thereunder, the rules of any designated contract market to which such AT Person submits orders through Algorithmic Trading, the rules of any registered futures association of which such AT Person is a member, the AT Person’s own internal requirements, or the requirements of the AT Person’s clearing member, in each case as applicable.

<sup>26</sup>See e.g., Regulation Systems Compliance and Integrity, 79 *Fed. Reg.* 72,252 (Dec. 5, 2014).

<sup>27</sup>*Id.*

Similarly, we believe the requirement to comply with the “requirements of the AT Person’s clearing member” is too general and broad. In addition, we are concerned that such standard lacks transparency. A clearing member may have requirements that are not based on legal or regulatory requirements but are for business purposes. An AT Person should not be expected to comply with such requirements, nor requirements or changes to requirements for which the AT Person is not aware. Unlike the rules of an SRO, a clearing firm’s requirements are not subject to administrative procedures that provide the public with an opportunity for notice and comment or due process. Further, without greater specificity, we are concerned that a requirement for an AT Person to comply with his clearing member’s requirements could constitute an unconstitutional delegation of authority. We believe it should be sufficient for an AT Person to comply with an AT Person’s obligations under Regulation AT and for an FCM clearing member to comply with an FCM’s obligations under Regulation AT. Contractual agreements between an AT Person and its clearing firm should remain contractual and enforceable by law by each signatory.

Finally, we believe the Commission should include a materiality standard in the definition of Algorithmic Trading Compliance Issue. A materiality threshold would better allow an AT Person to prioritize substantive issues and direct resources.

#### 4. Algorithmic Trading Disruption<sup>28</sup>

The term Algorithmic Trading Disruption is used with respect to Regulation AT’s pre-trade risk and other control requirements for AT Persons.<sup>29</sup> We believe that the definition of Algorithmic Trading Disruption should exclude “the Algorithmic Trading of such AT Person” and focus on *material* disruptions and *material* degradations by an AT Person to the operation of a DCM or the ability of other market participants to trade on such DCM.

Regulation should focus on the ability of the marketplace to operate as intended. By including a prong on the “Algorithmic Trading of such AT Person,” regulation focuses on whether an AT Person’s software is perfect at all times. It should not be a compliance violation for an AT Person to have a software glitch or hardware or data outage that does not impact a DCM or other market participants. AT Persons are motivated by their own self-interest to prevent systems issues. Given limited resources, we believe that regulators should concentrate resources on market events rather than individual events—such as, where an AT Person experiences a systems disruption and is unable to trade for a few minutes or more, particularly where such AT Person does not have an obligation to trade (*i.e.*, the AT Person is not a market maker).

---

<sup>28</sup>See Proposing Release at 78,937. § 1.3(uuuu), *Algorithmic Trading Disruption*. This term means an event originating with an AT Person that disrupts, or materially degrades—

- (1) The Algorithmic Trading of such AT Person,
- (2) The operation of the designated contract market on which such AT Person is trading, or
- (3) The ability of other market participants to trade on the designated contract market on which such AT Person is trading.

<sup>29</sup>See Proposing Release at 78,842.

Similarly, we believe the Commission should focus resources on material disruptions and degradations. We appreciate that the definition includes a materiality standard for degradations in activity; however, we believe it should be extended to events that are disruptive as well. Otherwise, we are concerned that Algorithmic Trading Disruptions could include inconsequential disruptions.

Lastly, we note that it may not be apparent to an AT Person whether it is impacting the ability of other market participants to trade on a DCM. This could be made clear by a tangible event, such as a notice by a DCM. The Commission could define an Algorithmic Trading Disruption *as an event originating with an AT Person that triggers a notice by a DCM, informing such AT Person that the event has materially disrupted or materially degraded (i) the operation of the DCM, or (ii) the ability of other market participants to trade on the DCM on which the event occurred.*

#### 5. Algorithmic Trading Event<sup>30</sup>

Regulation AT includes the use of the term “Algorithmic Trading Event,” which refers to an event at an AT Person that causes an Algorithmic Trading Compliance Issue or an Algorithmic Trading Disruption. Given our recommendations with respect to the definition of Algorithmic Trading Compliance Issue, we believe the term Algorithmic Trading Event is unnecessary and redundant. Should the Commission adopt the AT Person concept under Regulation AT, we believe it would be sufficient for § 1.81 to reference an Algorithmic Trading Disruption. Accordingly, the Commission should simplify Regulation AT by eliminating the unnecessary term Algorithmic Trading Event.

#### 6. Direct Electronic Access<sup>31</sup>

We believe the definition of “Direct Electronic Access” under Regulation AT is ambiguous. We understand that many market participants, including fundamental traders, connect to DCMs through exchange provided software or software provided by ISVs. We do not believe market participants using exchange-sponsored or ISV software to connect to a DCM should be considered as DEA participants.

In addition, we are concerned that the DEA term itself is contrary to how the term is used and understood with respect to § 38.607 and § 48.2,<sup>32</sup> which indicate that a market

---

<sup>30</sup>See Proposing Release at 78,937. § 1.3(vvvv), *Algorithmic Trading Event*. This term means an event at an AT Person that constitutes—

- (1) An Algorithmic Trading Compliance Issue; or
- (2) An Algorithmic Trading Disruption.

<sup>31</sup>See Proposing Release at 78,937. § 1.3(yyyy), *Direct Electronic Access*. This term means an arrangement where a person electronically transmits an order to a designated contract market, without the order first being routed through a separate person who is a member of a derivatives clearing organization to which the designated contract market submits transactions for clearing.

<sup>32</sup> CFTC § 38.607, Direct Access, provides: A designated contract market that permits direct electronic access by customers (i.e., allowing customers of futures commission merchants to enter orders directly into a designated contract



participant is trading through an FCM's fiber optic cables. We believe it is important for the Commission to use distinct terms with respect to Regulation AT and §§ 38.607 and 48.2.

We believe the Commission should clarify that the term DEA refers to situations where a market participant is not using exchange-sponsored or ISV provided software, and distinguish the definition from how it is used under existing §§ 38.607 and 48.2 by choosing another name.

### ***B. Proposed Risk Controls***

We believe the intention of proposed § 1.80 regarding pre-trade risk controls for AT Persons is to address execution system risk controls. It would be helpful for the Commission to clarify this understanding, as we found the requirement for AT Order Messages to have pre-trade risk controls ambiguous. The Commission could use a narrower definition of AT Person, such as MFA's proposed definition, which would make clear that the proposed pre-trade risk controls only apply to execution algorithms/systems.<sup>33</sup> If the Commission uses the definition of AT Person, as proposed, it should make clear that under § 1.80 an AT Person should use an execution system—whether its own or a third party's system—that includes certain risk-control features. We believe the Commission should make clear that an AT Person does not need to incorporate the proposed § 1.80 pre-trade risk controls into an investment algorithm, as we do not believe such controls are applicable to investment algorithms.<sup>34</sup>

In the Proposing Release, the Commission proposes “as a fundamental element of Regulation AT” a new requirement for AT Persons to implement measures reasonably designed to prevent an Algorithmic Trading Event, including:

- (a) maximum AT Order Message frequency;

---

market's trade matching system for execution) must have in place effective systems and controls reasonably designed to facilitate the FCM's management of financial risk, such as automated pre-trade controls that enable member futures commission merchants to implement appropriate financial risk limits. A designated contract market must implement and enforce rules requiring the member futures commission merchants to use the provided systems and controls.

CFTC § 48.2 defines *Direct access* to mean an explicit grant of authority by a foreign board of trade to an identified member or other participant located in the United States to enter trades directly into the trade matching system of the foreign board of trade.

<sup>33</sup> See *supra* Section IV.A.2.

<sup>34</sup> It would not be effective to require standardized pre-trade risk controls with respect to investment algorithms. First, orders generated by investment algorithms are always sent to a DCM through the use of an execution algorithm, which would incorporate the Proposed Controls under Regulation AT. Second, the Proposed Controls are not applicable to investment algorithms as the function of such algorithms are to determine what contracts to buy and sell as part of the investment or hedging strategy. Execution algorithms determine trade order parameters, such as the criteria in proposed § 1.80, including size, frequency, and price. Requiring investment algorithms to incorporate unnecessary and extraneous risk controls could increase the risk of errors while serving no beneficial purpose. Third, proprietary strategies of investment algorithms vary to such a great extent that it would be very difficult to standardize specific controls across such algorithms. Moreover, mandating unnecessary or inappropriate controls could actually increase market risk.

- (b) maximum execution frequency per unit time;
- (c) order price parameters;
- (d) maximum order size limits;
- (e) order cancellation systems;
- (f) Algorithmic Trading disconnect systems; and
- (g) connectivity monitoring systems for AT Persons with DEA

(the list of controls referred to together as the “**Proposed Controls**”). Generally, we believe the proposed § 1.80 pre-trade risk controls would be appropriate with respect to execution algorithms or execution systems (or as we have defined, an “AT System”).

In the electronic trading environment, all orders, whether generated through manual processes or through investment algorithms, or by registered or unregistered persons, are sent to the marketplace via an execution algorithm.<sup>35</sup> Market participants access the futures markets in a number of ways:

- A market participant may send its orders to a DCM through an FCM and use the FCM’s execution algorithm.
- A market participant may send its orders to a DCM through an FCM and use its own execution algorithm.
- A market participant may send its orders to a DCM through an FCM-sponsored ISV and use the ISV’s execution algorithm.
- A market participant may send its orders directly to a DCM, using the DCM’s software and execution algorithm.
- A market participant may send its orders to a DCM through a DCM-sponsored ISV and use the ISV’s execution algorithm.
- A market participant may send orders directly to a DCM, using its own proprietary execution algorithm.

---

<sup>35</sup> We continue to believe that it would be more effective to have centralized marketplace risk controls or marketplace requirements. By regulating certain categories of market participants rather than the activity, the Commission leaves open the possibility of an unregistered person causing a marketplace disruption by submitting an order through a third-party execution system that does not meet the Commission’s standards.

Consistent with industry practice, we believe it is critical to have risk controls at the execution algorithm-level, and that the types of controls Regulation AT proposes would be appropriate provided that market participants are able to personalize their own parameters.

*C. Development and Testing Requirements for Algorithmic Trading Systems*

MFA appreciates that the Commission is trying to standardize principles and procedures to reduce the operational risk of algorithmic trading systems. Nevertheless, we are strongly concerned with the one-size-fits-all nature of Regulation AT, and believe that it is not proportionate or scalable with respect to different types of registrants and the sizes of their operations. We are concerned that the prescribed requirements under proposed § 1.81(a) are not appropriate or suitable across a broad and diverse industry. Moreover, we are concerned that adopting regulations prescribing development and testing standards will not allow industry development and testing standards to evolve and improve with new technologies.

We have a number of concerns with proposed § 1.81 and its applicability under Regulation AT to CTAs and CPOs, and in this respect, provide a number of comments and suggestions below to illustrate our point. We believe, at most, the Commission should include under proposed § 1.81, development and testing practices for an AT Person to consider “where appropriate,” rather than for an AT Person to establish as minimum standards.

Proposed § 1.81(a)(1)(i) requires an AT Person to maintain a development environment that is adequately isolated from the production trading environment.<sup>36</sup> We believe the Commission should clarify that physical separation is not necessary. For a smaller-scale business, physical separation may not be feasible. Also, CTAs/CPOs may operate several different strategies, and, similarly, it would not be feasible to have separate sets of computers, networks, and databases for each strategy’s development and production environments. We believe CTAs/CPOs should be allowed to implement virtual separation rather than physical separation for software development and production trading. In addition, there may be elements that AT Persons want to share between development and production environments, such as market data infrastructure or reference data files.

We believe the purpose of § 1.81(a)(1)(i) is to ensure that an entity has procedures in place to develop and test software prior to use, and that software changes are not implemented during live trading. We believe this objective can be achieved in a more scalable manner and without requiring physical separation. Accordingly, we would suggest that the Commission amend § 1.81(a)(i) to require an AT Person to have separate development and production phases/procedures.

---

<sup>36</sup> Proposing Release at 78,938. Proposed § 1.81(a)(1)(i) requires: Maintaining a development environment that is adequately isolated from the production trading environment. The development environment may include computers, networks, and databases, and should be used by software engineers while developing, modifying, and testing source code.

Proposed § 1.81(a)(1)(ii) requires an AT Person to test all Algorithmic Trading code prior to implementation.<sup>37</sup> We are concerned that this requirement is too broad and believe that it should be limited by a materiality standard. It is not uncommon for CTAs and CPOs to make minor adjustments to certain parameters embedded in their investment trading software on a daily basis, including administrative changes, or enhancements. Systematic CPOs and CTAs, for example, may trim minor aspects of their code to accommodate factual changes (*e.g.*, a new bank holiday or early closing in a domestic or an overseas market; new position limits for individual positions) or make small adjustments to alpha generation (*e.g.*, using a 29 day moving average instead of a 30 day moving average as a strategy baseline). Different CPOs and CTAs have different concepts of materiality for higher-level signoffs and the proposed Regulation AT could require a one-size-fits-all *de minimis* threshold.

Requiring full-scale testing for any software modification, regardless of the materiality of the change, would make it cost-prohibitive for a market participant to regularly implement changes. In fact, such a requirement could have the unintended consequence of deterring market participants from implementing or delaying the implementation of software updates, modifications or changes by adding a cost component. We are concerned that such an environment could create unnecessary market risk. Instead, we would suggest that the Commission modify the testing requirement under § 1.81(a)(1)(ii) by adding a materiality standard.

Proposed § 1.81(a)(1)(iii) requires an AT Person to conduct regular back-testing of Algorithmic Trading.<sup>38</sup> Back-testing of trading software is a common and prudent industry practice with respect to a new trading algorithm. It is unclear what the Commission aims to achieve through *regular* back-testing of trading software as this serves no additional purpose. Upon back-testing a new trading algorithm, a market participant learns how the trading algorithm would perform. Re-testing will not change the results or how the trading algorithm performs; and once the trading algorithm is used live, the market participant will have live/actual results. Thus, we would suggest that the Commission amend § 1.81(a)(1)(iii) to require that an AT Person conduct back-testing of *new* trading algorithms prior to use in a live trading environment.

Proposed § 1.81(a)(1)(iv) requires an AT Person to conduct regular stress tests of Algorithmic Trading systems.<sup>39</sup> This requirement isn't suitable for all Algorithmic Trading systems. For example, we believe it is important for a DCM to ensure that it conducts stress tests of its trading systems to ensure capacity, integrity and resiliency. Similarly, it may be reasonable for a market participant operating an execution algorithm/system to conduct stress tests to ensure

---

<sup>37</sup> Proposing Release at 78,938. Proposed § 1.81(a)(1)(ii) requires: Testing of all Algorithmic Trading code and related systems and any changes to such code and systems prior to their implementation, including testing to identify circumstances that may contribute to future Algorithmic Trading Events. Such testing must be conducted both internally within the AT Person and on each designated contract market on which Algorithmic Trading will occur.

<sup>38</sup> Proposing Release at 78,938. Proposed § 1.81(a)(1)(iii) requires: Regular back-testing of Algorithmic Trading using historical transaction, order, and message data to identify circumstances that may contribute to future Algorithmic Trading Events.

<sup>39</sup> Proposing Release at 78,938. Proposed § 1.81(a)(1)(iv) requires: Regular stress tests of Algorithmic Trading systems to verify their ability to operate in the manner intended under a variety of market conditions.

it can continue to provide clients with execution services under a variety of market conditions (*i.e.*, during times of market stress with a high level of incoming orders). For a market participant operating an investment algorithm, however, the requirement to stress test an Algorithmic Trading system is not particularly meaningful. Generally, CTAs and CPOs conduct risk testing and risk management of their investment strategies or systems testing for business continuity purposes; but it is not clear how they would stress test an investment algorithm—investment software that analyzes data to determine whether to buy or sell. Thus, we would suggest that the Commission amend § 1.81(a)(1)(iv) to limit the requirement to conduct stress tests to AT Persons operating execution algorithms or to require stress tests in the context of business continuity planning.

Proposed § 1.81(a)(1)(v) requires an AT Person to have procedures for documenting the strategy and design of proprietary Algorithmic Trading software and changes to such software.<sup>40</sup> We believe this requirement is unnecessary and redundant due to our source code preservation recommendation below. We also believe proposed § 1.81(a)(1)(v) would be burdensome and add an additional and unnecessary layer of books and records requirements. CTAs and CPOs engaged in algorithmic trading are constantly revising and improving their algorithms. Proposed § 1.81(a)(1)(v) would require separate documentation of every code change, which would already be captured by a CTA's/CPO's source code management system.

In addition, MFA is strongly concerned that a requirement to maintain as books and records and to produce “white papers” or other design documentation presents a serious intellectual property risk. A good design document could provide another programmer with enough information to replicate a good portion of a proprietary strategy. In some ways, proposed § 1.81(a)(1)(v) presents even more of a risk than the source code retention requirement (discussed below), as it could remove the need to reverse-engineer raw source code by supplying what is – in essence – an instruction manual.

In balancing regulators' need for information with market participants' need to protect intellectual property, we believe a source code retention requirement strikes an appropriate balance and makes proposed § 1.81(a)(1)(v) unnecessary.

#### ***D. The Source Code Retention Requirement***

Chairman Massad explained at a recent Commodity Futures Trading Commission Budget hearing:

What we were trying to do was to make sure that what we call the source code for automated trading . . . is preserved. . . . When you have a problem . . . you need to go back and look at that source code to figure out what happened, and because firms change their algorithms from time to time, the current source code might be different than from what it was 6 months ago when the incident happened. . . . So

---

<sup>40</sup> Proposing Release at 78,938. Proposed § 1.81(a)(1)(v) requires: Procedures for documenting the strategy and design of proprietary Algorithmic Trading software used by an AT Person, as well as any changes to such software if such changes are implemented in a production environment.

what we're asking is simply that they preserve it – so if there's a problem, we can look at it and . . . reconstruct events.<sup>41</sup>

In light of Chairman Massad's objective behind proposed § 1.81(a)(vi),<sup>42</sup> we believe his concern may be addressed in a more targeted and balanced fashion through a source code retention requirement. While we have strong concerns with the source code inspection requirement under proposed § 1.81(a)(vi), as discussed below, we support the requirement that AT Persons maintain versions of the source code for five years. MFA recognizes the need for a preservation requirement to ensure that source code and any audit trails that are relevant to a given investigation are preserved and made available to the Commission (and other agencies referenced below) when appropriate. Accordingly, we recommend that the Commission narrow the scope of proposed § 1.81(a)(vi) to only include a source code retention requirement.

### *E. Intellectual Property Concerns*

#### 1. Source Code Repository Requirement

Proposed § 1.81(a)(1)(vi) requires AT Persons to maintain a source code repository to manage source code access, persistence, copies of production code, and changes to production code. It also, by reference to CFTC § 1.31, requires AT Persons to maintain versions of the source code for five years and make it available for inspection by the Commission or the Department of Justice (the “DOJ”) upon request and without a subpoena.

We recognize the need, in the appropriate circumstances, for the Commission, other regulators and self-regulatory authorities, federal prosecutors, and law enforcement agencies to be able to obtain and review confidential, proprietary material that trading firms and other businesses maintain. We also understand the need for a preservation requirement that will ensure that the source code and any audit trails that are relevant to a given investigation be preserved and be made available to the Commission (and the other agencies referenced above) when appropriate.

However, this modest proposal is, in fact, a monumental source of risk, anxiety and exposure for many MFA members. Algorithmic managers have all or substantially all of their enterprise value embedded in their code. We are strongly concerned with the proposed requirement that it be made available to regulators and prosecutors upon request, *with no need to allege or make a showing of manipulation, fraud or other wrongdoing*. While we have no doubt that the Commission, the NFA, and the DOJ will take what they consider to be reasonable

---

<sup>41</sup> See response by Timothy Massad, Chairman, CFTC at the Hearing before the House Agriculture Committee and Agriculture Appropriations Subcommittee on the Budget of the Commodity Futures Trading Commission, February 10, 2016.

<sup>42</sup> Proposing Release at 78,938. Proposed § 1.81(a)(1)(vi) requires: Maintaining a source code repository to manage source code access, persistence, copies of all code used in the production environment, and changes to such code. Such source code repository must include an audit trail of material changes to source code that would allow the AT Person to determine, for each such material change: who made it; when they made it; and the coding purpose of the change. Each AT Person shall keep such source code repository, and make it available for inspection, in accordance with § 1.31.

protective measures to protect the source code, regulated entities will have no transparency or knowledge of what those standards are and whether the government is following its own policies and procedures. In addition the simple fact is that government servers are in a constant state of cyberattack and that government systems have repeatedly been hacked or are exposed to electronic compromise, leads us to believe that government officials should not seek to take possession of highly proprietary information except in extraordinary circumstances.<sup>43</sup>

In fact, the CFTC Office of the Inspector General stated that for fiscal year 2016 the Commission's most serious management challenge is to

“Minimize information security vulnerabilities in its network. In light of the extent of information security vulnerabilities we identified this period, the Chief Information Security Officer is using his authority and resources to drive actions for effective vulnerability management.”<sup>44</sup>

More recently, President Barack Obama acknowledged that, “the federal government—which is obligated to protect the information provided to it by the American people—has a unique responsibility to lead. But the fact is we still don't have in place all the tools we need”.<sup>45</sup>

MFA recognizes (and actively supports) the need for the Commission and NFA to have access to trading information in the event of a market event, to have enough information about a manager's trading strategy to be able to effectively regulate and protect the futures, options and swaps markets. However, there are more useful and less intrusive methods by which the Commission can oversee markets, whether it is to investigate a market event, or to examine and verify that a market participant's code is legitimate or to test its resilience.<sup>46</sup>

---

<sup>43</sup>See e.g., Patricia Zengerle and Doina Chiacu, “Head of hacked U.S. agency says problems ‘decades in the making,’” *Reuters* June 16, 2015); Elizabeth Weise, “U.S. Postal Service hacked, told Congress Oct. 22,” *USAToday* (Nov. 10, 2014) (available at <http://www.usatoday.com/story/tech/2014/11/10/us-postal-service-post-office-hacked/18795289/>); Sarah Lynch, “SEC's information technology at risk of hacking: report,” *Reuters*, (Apr. 17, 2014); John P. Mello Jr., “Pentagon: Yep, We Got Hacked,” *TechNewsWorld* (Aug 26, 2010);

<sup>44</sup> See CFTC Office of the Inspector General Report, October 26, 2015, regarding the Inspector General's Assessment of the Most Serious Management Challenges Facing the Commodity Futures Trading Commission, available at: <http://www.cftc.gov/idc/groups/public/@aboutcftc/documents/file/oigmgmtchall2015.pdf>.

<sup>45</sup> See also President Barack Obama, "Protecting U.S. Innovation From Cyberthreats," *Wall Street Journal*, Feb. 9, 2016, available at: <http://www.wsj.com/articles/protecting-u-s-innovation-from-cyberthreats-1455012003>.

<sup>46</sup> Examiners could, for example, provide a manipulated dataset and require that the manager's systems be run against it to demonstrate these points.

2. The Goals of the Source Code Inspection Requirement are Already Satisfied Through Existing Legal Mechanisms

Instead of pursuing the source code inspection requirement, we urge the Commission to use the legal mechanism that already exists for obtaining and reviewing source code – and other confidential, proprietary information – *i.e.*, the subpoena process.

Under current law and practice, obtaining a subpoena allows the Commission (or any other regulator or prosecutor) to access and review source code, any associated audit trail, and other documentary evidence – all this with only a modest increase in the effort required in making a demand of an AT Person (as is contemplated in the Proposed Rule).<sup>47</sup> The Commission routinely uses its broad subpoena power to investigate trading activities and seek communications, data, and other information, even requiring that subpoena responses comply with the Commission’s own data delivery standards.

(a) *The Existing Subpoena Process is more Efficient and Effective than the Proposed Source Code Inspection Requirement*

As a practical matter, when regulated entities receive subpoenas, or are notified that they can be provided a subpoena if necessary, they often agree to produce the information voluntarily. (In fact, this has become a widely accepted practice in any investigation of a corporate entity.) Even where a subpoena is served, most government agencies, including the Commission, generally begin the subpoena process with a fairly broad request that seeks more information than the agency actually wants to review; however, a subpoena often opens up a dialogue between the agency and the subpoena recipient, typically resulting in the recipient producing information on a rolling basis.<sup>48</sup> This allows the agency to narrow the subpoena and obtain exactly what it needs, without wasting time and resources wading through irrelevant data.

MFA believes that – in any given situation – the existing subpoena process is much more likely to yield the type of information that the Commission will find useful. By contrast, the source code requirement may simply result in a “data dump” that would not be as useful to the Commission in its efforts to investigate and regulate problematic trading activity. Combined with the preservation requirement, which will guarantee that the information is available when a subpoena is issued, there is nothing the Commission (or any other regulator or law enforcement agency) would gain from the Proposed Rule that cannot be obtained through the existing subpoena.

(b) *The Existing Subpoena Process Offers Significant Additional Protection for Intellectual Property without Diminishing the Commission’s Effectiveness*

In addition, the subpoena process would assuage many of the concerns that MFA members have regarding the source code inspection requirement in the Proposed Rule. The

---

<sup>47</sup> See Section 6(c) of the Commodity Exchange Act; and CFTC § 11.4, Subpoenas.

<sup>48</sup> Often, the recipient of a subpoena will agree to cooperate further, by making a “proffer” or other oral presentation to assist the agency in narrowing its subpoena and furthering its investigative goals.



subpoena process offers CPOs/CTAs legal protection, in the ability to seek a protective order or other negotiated confidentiality agreement, to make sure that the confidentiality of their source code is properly maintained.

This ability to safeguard the source code is critical to firms that seek to protect their source code under state and federal trade secrets laws. These laws generally require that the owners of trade secrets take steps to maintain confidentiality – otherwise, the information may not be legally recognized as a trade secret – a result that would be devastating to firms that have invested millions of dollars in developing their proprietary source code.

The subpoena process would allow the Commission and CPOs/CTAs to reach a mutually acceptable arrangement on the secure preservation of source code. The parties could, for example, agree to set up a secure system at a manager's office for on-demand review of necessary source code, or could agree on temporary retention measures (including security and cybersecurity measures) for the Commission's personnel to have off-site access.

### 3. The Source Code Inspection Requirement Creates Risks of Downstream Disclosures

Another danger of the source code requirement is the Commission's (and the NFA's) ability to keep the information confidential from third parties. MFA is concerned about a number of potential issues on this topic:

*First*, as discussed above, government servers are vulnerable to cyberattacks and are routinely targeted by domestic and foreign cybercriminals. Despite the Commission's best intentions to protect the source code, a cyberattack is a real possibility and the consequences for our members who made their source code available would be disastrous.

*Second*, while we anticipate that the Commission would be able to assert (on numerous grounds) that the source code is exempt from the Freedom of Information Act<sup>49</sup> (“FOIA”), we are concerned that it is not a certainty. FOIA requests, even narrowed FOIA requests, could easily put MFA members' intellectual property at risk. In addition, there is always the risk of human error in maintaining the confidentiality of a registrant's source code.

*Third*, the Commission may face Congressional demands for information. We believe that the Commission would be unable to refuse a Congressional demand for a given MFA member's (or, indeed, for *all* of MFA's systematic manager members') source code on a FOIA basis. Instead, the CFTC would likely be required to produce the information to Congress, which would exercise its own discretion about whether to disclose the information to the public.<sup>50</sup> Naturally, the Commission would be far less suited (or incited) to argue that the source code should be kept confidential, than the owner of the source code who developed it. (And recent

---

<sup>49</sup> 5 U.S.C. § 552.

<sup>50</sup> While this risk is not completely obviated by the use of the subpoena process, we believe that Congress is very unlikely to seek production of material that was produced under a negotiated (and perhaps court-approved) production process.

history has shown that Congress can at times be than less rigorous in respecting the confidentiality of regulatory submissions.<sup>51</sup>)

*Fourth*, we have other downstream disclosure concerns with leaving the source code in the hand of NFA. NFA is not a governmental organization, and it is subject to all matter of suits and other legal process. While we expect that NFA will act responsibly and carefully in handling these other legal matters, we believe that decisions on disclosure of MFA members' valuable, confidential intellectual property should remain solely in the hands of the MFA members.

We also have concerns with the ability of third party contractors to maintain the confidentiality of source code and other proprietary information to the extent that the Commission or other regulators need to use outside expertise to maintain or understand a registrant's proprietary information. So-called "source code escrows" have been proposed and re-proposed as solutions to a host of concerns and risks – from bankruptcy and secured lending to disaster recovery – but both history and current practice demonstrate that the use of third-party source code escrows is problematic, and their use remains fairly uncommon. Accordingly, the source code escrow agents that are in operation are largely unregulated, generally act without common standards or certifications, and may not be subject to fiduciary obligations. MFA members would also be extremely concerned – on both cybersecurity and more general trade secret protection grounds – at the prospect of being forced to escrow code with such a third party.

#### 4. The Commission Can Achieve its Goals Through Preservation Requirements

If the source code repository concept is to be maintained, MFA proposes that instead of leaving the term "source code repository" undefined and ambiguous, the Commission instead clarify that by the use of this term the Commission is merely requiring that AT Persons implement systems that provide for:

- (a) the preservation (on par with other preservation requirements for certain categories of books and records) of the source code utilized for algorithmic trading;
- (b) a mechanism for producing current and prior versions of such source code; and
- (c) a mechanism for tracking material changes to the source code.

Note that we are proposing that the Commission adopt mechanisms for producing prior versions of the source code and mechanisms for tracking material changes rather than

---

<sup>51</sup> See, e.g., Gregory Meyer, "Senator's Leak Sparks Commodities Debate," *Financial Times* (August 21, 2011) (available at <http://www.ft.com/intl/cms/s/0/645a8228-caad-11e0-94d0-00144feabdc0.html>) ("Last week Bernie Sanders, a Vermont independent, leaked and later posted on his website lists of trading positions in oil, natural gas and other commodity markets as part of a campaign to force a clampdown on commodity speculation.")

archived prior versions. While it is technically possible to keep “snapshots” of prior versions of code, to do so in a change-indexed environment is actually a daunting logistical endeavor. While archived snapshots are kept for disaster recovery reasons, they generally are not indexed to changes in a manner that would be useful to the Commission. Market practice is to have current versions that have embedded notes and histories to demonstrate past changes.

MFA believes that the use of a straightforward, enumerated set of obligations would better serve the market as a whole; as it would allow market participants to make independent decisions on the highest security storage and indexing methods, the most convenient and effective means of indexing; the best storage media, and the most effective provider of these functions (which could include an in-house storage solution).

#### ***F. Enhancing Information Security Protections at Regulators***

MFA and its members are concerned with the high risk and threat of cyberespionage. The General Accounting Office found that federal agencies had 67,168 cybersecurity incidents in 2014 alone—a 1,121% increase since 2006.<sup>52</sup> In Congressional testimony in 2014, the FBI’s Assistant Director charged with cybersecurity said that every federal agency has been the victim of cyberespionage.<sup>53</sup> As noted earlier, the CFTC Office of the Inspector General has cited the Commission for information security vulnerabilities associated with the vast majority of servers and network users.<sup>54</sup> Whether requesting source code or maintaining the confidentiality of existing non-public information with respect to market participants, we believe the CFTC and other regulators need to enhance their information security policies and procedures for safeguarding confidential information of market participants.

Market participants go to great lengths to protect sensitive intellectual property. Many of the practices are shaped by case law from intellectual property cases. Below are some common practices by investment professionals:

1. Maintaining an inventory of personally identifiable information, trade secrets, and other sensitive information.
2. Logging each time sensitive information is accessed, and by whom.

---

<sup>52</sup> Gregory C. Wilshusen, Director, Information Security Issues, Testimony before the Subcommittee on Research and Technology Oversight, Committee on Science, Space, and Technology, House of Representatives, 7 (July 8, 2015), available at <http://www.gao.gov/assets/680/670935.pdf>.

<sup>53</sup> See Public Statement of Luis A. Aguilar, Commissioner, SEC, on “Being a Responsible Steward: Ensuring that the SEC Implements Effective Cybersecurity Protocols for its Data Gathering Efforts,” Dec. 16, 2015, (citing James Cook FBI Director) available at: <https://www.sec.gov/news/statement/being-a-responsible-steward-cybersecurity.html>. See also James Cook, FBI Director: China Has Hacked Every Big US Company, Business Insider (Oct. 6, 2014), available at <http://www.businessinsider.com/fbi-director-china-has-hacked-every-big-us-company-2014-10>.

<sup>54</sup> See *supra* n. 9; see also Office of the Inspector General, CFTC, Semiannual Report to Congress, April 1, 2015 – September 30, 2015, available at: [http://www.cftc.gov/idc/groups/public/@aboutcftc/documents/file/oig\\_reporttocongress093015.pdf](http://www.cftc.gov/idc/groups/public/@aboutcftc/documents/file/oig_reporttocongress093015.pdf).

3. Maintaining safeguards to protect sensitive information, including:
  - Restricting access to and use of areas/equipment/information;
  - Use of separate servers;
  - Use of physical locks and passcodes;
  - Use of security cameras;
  - User access controls (“UAC”) (*i.e.*, restricting user access to files based on need to know; read-write privileges on a per user or group basis)
  - Limiting use of portable storage devices and access to the internet with systems that contain sensitive information;
  - Developing protocols for sharing/transferring data;
  - Use of private source code repository (*i.e.*, source code management); and
  - Making programming code difficult to reverse engineer.
4. Requiring employees to sign confidentiality obligation, nondisclosure agreements, (“NDA”) and adhere to strict policies and procedures.
5. Limiting disclosure to third parties and requiring NDAs when revealing any confidential information.

Given the level of confidential and proprietary information that the CFTC and other regulators maintain and/or are able to access, we strongly urge the CFTC, NFA and other regulators to promptly adopt additional protocols to protect confidential information. Information security vulnerabilities at a regulator could jeopardize not only market participants and their investors, but the U.S. economy through the loss of domestic trade secrets and confidence in the integrity of the regulatory framework. MFA recommends that the CFTC, and other regulators, at a minimum, ensure that they have protocols to:

- Restrict how and where staff obtain (or maintain) access to sensitive information;
- Limit and document staff access to sensitive information;
- Implement safeguards to protect intellectual property that are equivalent to industry best practices;
- Conduct regular staff training on policies and procedures with respect to protecting confidential information; and
- Inform and remind employees and former employees of post-employment obligations.

Our comments are not just restricted to governmental entities. NFA obviously plays a key role in the futures and options markets, and we would advocate for NFA to undertake, either voluntarily or through a mandate from the Commission, the same proactive measures that we propose for the Commission.

## ***G. Monitoring, Compliance and Training Regarding Algorithmic Trading Systems***

### **1. Monitoring of Algorithmic Trading Systems**

MFA supports requiring an AT Person to have policies and procedures with respect to monitoring an algorithmic trading system. However, we do not believe the specific monitoring requirements under proposed § 1.81(b) are appropriate for all types of Algorithmic Trading. Similar to our comments regarding proposed § 1.81(a)(1), we believe it would be best for the Commission to require that market participants have policies and procedures for monitoring Algorithmic Trading systems but to allow market participants to determine the most appropriate manner in which to monitor their systems.

Proposed § 1.81(b)(i) requires an AT Person to have policies and procedures regarding continuous real-time monitoring of Algorithmic Trading. Many investment algorithms, however, do not operate continuously throughout the trading day. A CTA's or CPO's investment algorithm may provide the CTA or CPO with orders each morning to send to an FCM for execution before the market opens and then be finished for the day. As Algorithmic Trading systems may not be in continuous operation, we do not believe it is appropriate to require continuous real-time monitoring of such systems. Similarly, we do not believe it is necessary under proposed § 1.81(b)(iv) to require procedures that will enable AT Persons to track which monitoring staff is responsible for an Algorithmic Trading system during trading hours, as some investment algorithms may not operate during trading hours. Even with respect to Algorithmic Trading systems that operate throughout the day, we believe the Commission should provide all AT Persons with flexibility in determining how they monitor their systems and track monitoring staff.

Proposed § 1.81(b)(ii) requires an AT Person to have policies and procedures regarding automated alerts when an Algorithmic Trading system's AT Order Message behavior breaches design parameters, upon loss of network connectivity or data feeds, or when market conditions approach the boundaries within which the Algorithmic Trading system is intended to operate. Generally, algorithms are designed to simply shut-off when design parameters are breached.<sup>55</sup> As such, we believe it's unnecessary to prescribe that an Algorithmic Trading system have automated alerts. We strongly believe an AT Person should have discretion with respect to when an automated alert should be triggered, as alerts will become meaningless when there are too many or too easily triggered.

If the Commission determines to adopt the Regulation AT framework, MFA suggests that the Commission amend proposed § 1.81(b) to require each AT Person to have written policies and procedures, appropriately designed with respect to its trading and its business, to

---

<sup>55</sup> See, e.g., Aldrich, Grundfest and Laughlin, *The Flash Crash: A New Deconstruction*, January 25, 2016, available at: [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2721922](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2721922) (continuing with analysis to determine whether market data feed anomalies were a symptom of the rapid trading that accompanied the Flash Crash or whether they were causal in the sense that they rationally contributed to traders' decisions to withdraw liquidity and then restore it after the anomalies were resolved). See also, *Findings Regarding the Market Events of May 6, 2010*, Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues, September 30, 2010, available at: <https://www.sec.gov/news/studies/2010/marketevents-report.pdf> (explaining that market data feed delays could have directly triggered integrity-pauses in many automated trading systems).

reasonably ensure that knowledgeable and qualified staff monitor each of its Algorithmic Trading systems.

2. Compliance, Designation and Training with Respect to Algorithmic Trading Systems and Staff

We do not take issue with the obligation of all CPOs and CTAs to have training systems and informational outreach efforts. In fact MFA members often endorse these kinds of controls as best practices. However, we feel that designating, in a formal regulation, a training obligation for certain personnel is a radical departure from past precedent in the futures and in the securities markets. In addition, we are concerned that the specific requirements under proposed § 1.81(c) and (d) may not necessarily be appropriate in all circumstances. For example, § 1.81(c)(3) requires an AT Person to take *prompt* action to document and remedy deficiencies in its policies and procedures. However, there may be times when a firm believes that it would be more impactful to immediately address other risk-reducing measures rather than promptly remediate a gap in its policies and procedures. We believe that CPOs and CTAs have overall supervision obligations and fiduciary duties that provide the kind of protection that the Commission is seeking. We therefore, would respectfully urge that these provisions be dropped from any final regulation.

**H. AT Person Reports and Recordkeeping**

Proposed § 1.83 requires an AT Person to submit annual compliance reports, and books and records as requested, to each DCM on which it engages in Algorithmic Trading.<sup>56</sup> We have strong concerns with proposed § 1.83, as we believe it creates an unnecessarily burdensome and redundant regulatory framework. Instead, we believe the CFTC should require CTAs and CPOs, as part of their annual NFA Self-Examination Questionnaire, to describe and certify that they have appropriate risk controls in place tailored to their algorithmic trading systems.<sup>57</sup> Moreover, we are concerned that the proposed framework of requiring DCMs to oversee AT Persons through annual AT Reports would be inefficient and duplicative, as well as ineffective for ensuring that AT Persons have effective risk controls in place.

As discussed in Section IV.E, we have strong concerns with the proposed requirement to maintain source code as a books and records requirement. That aside, we are concerned in general with the Commission's reference under proposed § 1.81 to maintain records in accordance with § 1.31. MFA, jointly with the Investment Adviser Association and the Alternative Investment Management Association (together, the "**Associations**"), petitioned the Commission to modernize its recordkeeping requirements applicable to CPOs and CTAs by amending § 1.31.<sup>58</sup> The Associations are concerned that § 1.31 is outdated, burdensome, and

---

<sup>56</sup> Proposing Release at 78,939.

<sup>57</sup> See also, *supra* Section III.

<sup>58</sup> Letter to Melissa D. Jurgens, Secretary, CFTC, from Stuart Kaswell, General Counsel, MFA, Karen Barr, General Counsel, IAA, and Jiří Król, Deputy CEO, AIMA, dated July 21, 2014, regarding "Petition for Rulemaking to Amend CFTC Regulation 1.31, 4.7(b) and (c), 4.23 and 4.33" available at: <https://www.managedfunds.org/wp-content/uploads/2014/07/Final-Petition.pdf>.

exposes registrants to unnecessary and considerable risk by requiring the continued use of outdated technology. The Commission staff has also acknowledged concerns with § 1.31 and its applicability to the current technological environment.<sup>59</sup> We believe it is imperative for the Commission to amend § 1.31 before the Commission adopts Regulation AT.

### ***I. Self-Trade Prevention Tools***

Regulation AT provides that DCMs must establish self-trade prevention tools, and either apply such tools or provide them to market participants and require their use. “Self-trading” is proposed to be defined as the matching of orders for accounts with common beneficial ownership *or under common control*. DCMs would be required to either identify accounts that would be prohibited from trading with each other and/or require market participants to identify such accounts.

#### **1. MFA Advocates for a Self-Certification System**

We believe that a system that requires multiple parties to identify accounts that are related will create a costly burden on the marketplace. We worry that there will be multiple, inconsistent databases and databases that are internally inconsistent. In addition, we believe that this kind of a system represents a costly and inefficient way to handle this matter (and one that we are not sure was contemplated in the Commission’s cost-benefit analysis). Instead, we recommend that a self-trading CPO self-certification system be employed. This would be subject to verification on examination by the NFA and represents an efficient solution. (We note that this kind of approach works well in other Commission rulemaking areas.)

#### **2. MFA Believes that the Current Trade Surveillance System Works Well and Protects the Markets.**

MFA recommends that the Commission retain the current “self-trading” surveillance framework in lieu of the proposed framework under Regulation AT. We believe the existing self-trade surveillance framework functions well and is more than adequate in preventing self-trading in the markets. In fact, CME has stated that the level of self-trades in the market is a fraction of one percent.<sup>60</sup>

We are concerned that the new self-trading definition under Regulation AT, proposed § 40.23(a), includes matching of orders for accounts that are “under common control.”<sup>61</sup> The Commission’s stated impetus for this change is a concern that “a trade that results from the

---

<sup>59</sup> See CFTC Letter No. 14-114, dated September 8, 2014, regarding “Exemptive Relief to Use Additional Third-Party Recordkeepers in Commission Regulation 4.7(b)(4) and 4.23(c)” available at: <http://www.cftc.gov/idc/groups/public/@lrllettergeneral/documents/letter/14-114.pdf>.

<sup>60</sup> CME believes that the level of wash-trades in today’s markets are, in general, extremely low and well below 1% of all of the trades effected on DCMs subject to the Commission’s supervision. See, e.g., comments by Bryan Durkin, Chief Commercial Officer, CME Group, at the CFTC Technology Advisory Committee Meeting, Feb. 23, 2016 (stating that self-trades are down to a fraction of one percent of activity”).

<sup>61</sup> Proposing Release at 78,941.

matching of opposing orders both generated by a firm or a single or commonly owned account does not shift risk between different market participants.”<sup>62</sup>

There are many instances of situations where a “self-trade” is permissible, is not manipulative or distortive, and is in the best interests of clients or pool participants. For example:

- At times, CTAs and CPOs may have clients with investment programs or mandates, both algorithmic and fundamental, where an advisor needs to execute opposing trades for each client. If this situation arises as a result of a *bona fide* set of concurrent but independent investment decisions, this behavior should not be prohibited.<sup>63</sup> For example, Client A may have a narrow mandate and may be seeking exposure to a given commodity, and a dip in that commodity's related futures contracts may trigger a buy order. However, Client B may have a much broader portfolio, and the same market conditions might trigger a larger buy order in another security or commodity interest that would – in turn – trigger a sale order in the same commodity futures contract that Client A is buying in order to preserve a hedge. Clearly, there are two different rationales, and the proposed rule places the CTA or CPO in the position of having to force one client to accept a worse execution in order to avoid self-trading.
- In the systematic world, many managers devise algorithms and programs that look to profit on relationships. It is possible that two different algorithms, independently developed and operated by a common investment team, will see a single futures contract as linked to another component in two separate situations. In this case, a trading decision is not triggered by the inherent value of the contract, but rather by the relationship of the instrument to another element or elements of an overall trading strategy. In this kind of scenario, it would not be uncommon for the two different strategies to generate opposing instructions. Here, again, these are independent decisions, joined only by the fact that the CPO is running multiple models concurrently.<sup>64</sup>

MFA members support the need for anti-manipulative efforts and – as noted below – agree that the DCM is the appropriate venue for controls and protections. However, we believe that the creation of a new concept – self-trading through commonly controlled accounts – is vague, potentially overbroad, and ultimately unwarranted. In short, MFA believes (and we believe that we are not alone in this view) that the proposal on self-trade prevention is a solution to a problem that does not exist.

---

<sup>62</sup> Proposing Release, at 78,877.

<sup>63</sup> And, under current exchange rules, this is permitted other than where there is a manipulative intent or where the clients have common beneficial ownership.

<sup>64</sup> This could also result in, under the proposed Rule, a CPO being *forced to create a link* between two otherwise separate, independently operating, and disparate models to avoid triggering a self-trade violation. We do not think it is an exaggeration to state that the “under common control” concept would be an effective cap on the growth and diversification of many of our members.



MFA recommends that the Commission continue to monitor how the DCMs (and all trading entities as a whole) address the prevention of self-trades and similar behavior. To the extent that the situation deteriorates, then a rule like the proposed § 180(e) may be necessary, but at the moment it would be an unnecessary burden for CPOs and other trading entities.

3. MFA Believes that the Self-Trade Prevention Efforts are Properly Located at the DCM.

Independent of the discussion as to whether a new “self-trading” concept is needed to complement the existing wash trade prevention systems is the question of where these controls should reside. Proposed § 1.80(e) requires that, “to the extent that implementation of a DCM’s self-trade prevention tools requires calibration or other action by an AT Person, such AT Person must calibrate or take such other action as is necessary to apply such tools.”<sup>65</sup>

MFA believes that a decision to impose on market participants the responsibility to ensure that they are compatible with a DCMs system and effectively to shoulder the DCMs matching prevention responsibilities is a well-intentioned catalyst for negative results. We have several concerns with this responsibility:

*First*, we believe that there is no viable alternative to locating the anti-matching function at the DCM level. Other than the DCMs, no other market participants are able to see the complete order book and no other market participants are able to effectively block self- or wash trades. While it may be possible for CPOs such as some of MFA's larger members to design systems that will attempt to do this, this is a much more difficult task than it appears to be at first blush and it has direct and indirect costs and negative effects on market efficiency. Internalized CPO-level safeguards are not perfect and – more importantly – will never be perfect (especially for firms with concurrent electronic and voice trading capabilities and multiple portfolio managers). The DCMs, on the other hand, as the recipient of all orders, will always have a perfect, real-time view on matchable orders and the entire trading environment. They are not just the participant with the “last clear chance” to prevent a self-trade, but they are the *only* market participant with the ability to prevent all self-trades.<sup>66</sup> Given this asymmetry in the ability to effect a positive result, it seems only natural to locate these controls within the DCM itself.

*Second*, mandating that market participants utilize a DCM's trade-matching technology means that duplication latency is introduced into the system. We all expect that the DCMs will continue to operate self-trade prevention systems, and mandating a market participant

---

<sup>65</sup> Proposing Release at 78,854.

<sup>66</sup> To that end, we would encourage the Commission to require DCMs to expand their self-trade prevention functionality – in particular, requiring that such functionality work across clearing FCMs for a particular market participant (*i.e.*, where a market participant clears trades through more than one clearing FCM, a DCM’s self-trade prevention technology should work to block trades from that market participant whether it clears through the same clearing FCM or another, without blocking that market participant’s interaction with all other trading interest cleared through the relevant FCM). Absent this functionality, a CPO is forced to trade entirely with a single FCM in order to take advantage of the DCM self-trade prevention functionality, which greatly, and unnecessarily, increases risk to investors.

interface will simply duplicate that effort and delay the operation of an algorithmic trader's systems. Not having self-trade controls at the DCM level will be inefficient at best and extremely costly at worst.

*Third*, forcing market participants to incorporate DCM self-matching interface code into their systems creates a new systemic risk. In this age of malicious hackers and cyber-terrorists, mandating that all electronic traders incorporate identical code and/or interface with a trade control system that is *identical for all participants* creates significant risks for MFA members and for the market as a whole. It does not take a great amount of imagination to see how a hacker could use those mandate trade control (as opposed to mere access, as is the situation today) links to steal intellectual property from market traders, to cause unauthorized trades (perhaps on a massive scale) to be placed, or to deny access to the market in times of crisis.

*Fourth*, we believe that the proposal is very current and reflects state of the art technology at the DCM and the CPO level. However, we think that the very concepts of DCM access can and will evolve and change over time. Adoption of this interface concept could well reflect an anachronistic concept in five or ten years and require additional rule-making. Allowing the DCMs to manage proprietary systems that are defined only by the desired goal, on the other hand, may well be a more durable and flexible contribution to market stability.

*Finally*, having the self-trade prevention systems reside at the DCM is the fairest result; it would create a level playing field for all market participants. We recognize that this may be an unexpected argument, as many of our members would have a competitive advantage over trading entities with less capacity to engineer faster and more streamlined integration solutions. However, MFA and its members believe that in the long run DCM access on a fair and equitable basis benefits everyone.

#### ***J. DCM Disclosures on Market Maker and Trading Incentive Programs***

Proposed § 40.25 requires a DCM to provide additional public information regarding its market maker and trading incentive programs, restricts certain types of payments by a DCM in connection with such programs, and requires a DCM to perform surveillance of such programs to prevent abusive practices. MFA is supportive of proposed § 40.25 and believes that the requirements will provide investors and the broader public with more information and transparency into DCM market maker and trading incentive programs. We agree with the Commission that the DCM disclosure and surveillance requirements regarding these programs will support and enhance market integrity. We also believe they will enhance investor confidence in the U.S. futures markets. In addition, we believe that the Commission should require Swap Execution Facilities (“SEFs”) to make similar types of market maker and trading incentive program disclosures. Applying these transparency requirements to SEFs would level the playing field with DCMs, as DCMs may directly compete with SEFs by listing swaps or economically similar contracts.

## V. COST ESTIMATE FOR REGULATION AT

MFA believes that the costs associated with Regulation AT are likely to be significantly greater than the Commission's cost estimates. First, the breadth of the Regulation AT definitions are likely to capture many more market participants as AT Persons than the 420 persons that the Commission estimates.<sup>67</sup> Combined, there are 2,540 CTAs and CPOs registered with the Commission.<sup>68</sup> We believe that most, if not all, CTAs and CPOs use algorithmic trading execution systems. Even if only half of all CTAs and CPOs used an algorithmic trading execution system, there would still be at least 1,270 CTAs and CPOs-alone that would be AT Persons before including other registrant categories.

Second, given the prescriptive yet one-size-fits-all nature of Regulation AT, CTAs and CPOs would need to expend significant resources to modify their business practices, including adding potentially unnecessary processes, in order to comply with Regulation AT. The Commission also did not provide estimates for ongoing costs associated with many aspects of Regulation AT, such as with respect to risk controls, development, testing and monitoring requirements.<sup>69</sup>

MFA surveyed a cross-section of its members on the estimated costs relating to Regulation AT. The results from our survey on the estimated costs for a CTA or CPO to comply with Regulation AT are summarized in the table below. We also included a table below comparing the Commission's estimates with the average cost estimate from our survey. MFA members that fall under the definition of "AT Person" due to the use of a third party or independent software vendor's off-the-shelf trading/execution algorithm reported that they were unsure of the costs of overseeing a third party with respect to Regulation AT, and thus, did not provide estimates. MFA members that completed MFA's survey on Regulation AT included costs from the following departments: Technology and IT; Legal; Compliance; and Outside Counsel.

---

<sup>67</sup> See *supra* Section IV.A regarding the definition of Algorithmic Trading and AT Person.

<sup>68</sup> See NFA Membership Totals, available at: <https://www.nfa.futures.org/nfa-registration/NFA-membership-and-dues.HTML>.

<sup>69</sup> See *supra* Sections IV. B, C, G, H and I regarding proposed risk controls, development and testing requirements, monitoring, compliance and training requirements, AT Person reports and recordkeeping, and self-trade prevention tools.

**Estimated Regulation AT Compliance Costs Per CTA or CPO Entity**

	Risk Controls		Development, Testing & Monitoring		Written Policies & Record Keeping		AT Compliance Report	DCM SMP Waiver
	One-Time Cost	Annual Cost	One-Time Cost	Annual Cost	One-Time Cost	Annual Cost	Annual Cost	
<b>Range</b>	\$70,000 - \$500,000	\$10,000 - \$150,000	\$100,000 - \$3.807 MN	\$20,000 - \$1MN	\$10,000 - \$1.322 MN	\$5,000 - \$400,000	\$4,240 - \$100,000	\$3,810 - \$10,000
<b>Mean</b>	\$223,683	\$76,571	\$860,636	\$252,714	\$283,384	\$77,538	\$37,567	\$7,453
<b>Median</b>	\$220,833	\$78,000	\$550,000	\$124,000	\$150,000	\$28,750	\$30,000	\$8,000
<b>CFTC Estimate</b>	\$79,680	No Estimate	\$546,425	No Estimate	\$5,130	\$2,670	\$4,240	\$3,810

**Comparison of CFTC Estimates with MFA Estimates**

Regulation	Description	CFTC Estimate Cost per Entity	MFA Estimate Cost per Entity*
§ 1.80	Risk Controls	\$79,680	\$223,683
§ 1.83(c)	Recordkeeping	\$5,130	\$283,384
<b>Total AT Persons</b>		\$84,810	\$507,067
§ 1.83(a)	Submit compliance reports/written policies	\$4,240	\$37,567
§ 1.83(c)	Recordkeeping	\$2,670	\$77,538
§ 40.23	Submit approval requests to DCMs to forego self-trade controls	\$3,810	\$37,567
<b>Total AT Persons</b>		\$10,720	\$152,672

\*Using the average estimated cost from MFA's survey.

**VI. CONCLUSION**

MFA has strong concerns with Regulation AT, as proposed, and believes that its approach to addressing operational systems risks related to algorithmic trading is flawed. *First*, MFA recommends that in lieu of adopting Regulation AT, the Commission adopt regulation requiring centralized pre-trade risk controls at DCMs and clearing FCMs. We believe centralized

controls at the DCM and clearing FCM-levels would be highly effective in preventing marketplace disruptions. In addition, we believe the Commission should address other derivatives marketplace concerns identified in Regulation AT through separate rulemakings and in different stages.

*Second*, to the extent the Commission determines to adopt Regulation AT, MFA recommends that the Commission exclude CTAs and CPOs from Regulation AT. Instead, to address concerns relating to CTAs/CPOs, MFA recommends that the Commission direct NFA to promulgate CTA/CPO regulatory requirements on operational systems risk controls; and to report to the Commission on data that it collects from an amended CTA/CPO Self-Examination Questionnaire that includes questions on operational systems risk controls. If necessary, the Commission should amend its Part 4 regulations to address CTA/CPO operational systems risk concerns related to algorithmic trading in a manner suited for CTA and CPO businesses and operations.

Finally, to the extent that the Commission determines to proceed with a broad Regulation AT framework that applies to all categories and sizes of market participants and different types of algorithmic trading functions, MFA believes that the Commission needs to adopt a more flexible framework. The Commission should identify specific marketplace concerns with respect to algorithmic trading activities and require market participants to prevent marketplace disruptions by: (1) using execution systems with pre-trade risk controls (when and if using algorithmic execution systems); (2) adopting development and testing standards reasonably designed to prevent operational systems risks and marketplace disruptions; (3) retaining source code; and (4) adopting monitoring, compliance and training programs reasonably designed to prevent operational systems risks and marketplace disruptions.

\* \* \* \*

MFA appreciates the opportunity to provide comments and recommendations on the Regulation AT. We would welcome the opportunity to discuss our views on Regulation AT with the Commission or its staff in greater detail. If the staff has any questions, please do not hesitate to contact Jennifer Han or the undersigned at (202) 730-2600.

Respectfully submitted,

/s/ Stuart J. Kaswell

Stuart J. Kaswell  
Executive Vice President & Managing Director,  
General Counsel  
Managed Funds Association