June 24, 2016

Via Electronic Submission

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

Re: 17 CFR Parts 1, 38, 40, and 170 Public Staff Roundtable on Elements of Regulation Automated Trading; Reopening of Comment Period

Dear Mr. Kirkpatrick:

The Futures Industry Association ("FIA"), FIA Principal Traders Group ("FIA PTG"), Managed Funds Association (MFA), International Swaps and Derivatives Association ("ISDA") and SIFMA Asset Management Group ("AMG") (collectively, the "Group"[1]) appreciate the

[1] FIA is the leading trade organization for the exchange-traded and centrally cleared derivatives markets worldwide. FIA's membership includes international and regional banking organizations, clearing houses, exchanges, brokers, vendors and trading participants. FIA's mission is to support open, transparent and competitive markets, protect and enhance the integrity of the financial system and to promote high standards of professional conduct. Further information is available at www.fia.org.

FIA PTG is an association of 25 firms that trade their own capital on exchanges in futures, options and equities markets worldwide. FIA PTG members engage in manual, automated, and hybrid methods of trading, and they are active in a wide variety of asset classes, including equities, fixed income, foreign exchange and commodities. FIA PTG member firms serve as a critical source of liquidity, allowing those who use the markets, including individual investors, to manage their risks and invest effectively. FIA PTG advocates for open access to markets, transparency, and data-driven policy.

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

opportunity to provide additional comments on the Commodity Futures Trading Commission's ("CFTC" or the "Commission") Notice of Proposed Rulemaking on Automated Trading ("Reg AT" or the "NPR") during this re-opened comment period to address provisions of Reg AT raised in the June 10, 2016 public roundtable (the "Roundtable").

The associations comprising the Group filed comment letters during the initial comment period on the NPR (the "Initial Comment Letters"). The Group reiterates and incorporates its Initial Comment Letters herein.

Introduction

Since the initial comment period concluded, a wide variety of market participants, represented by the associations listed above, have been discussing various provisions of the NPR with the intent to provide the CFTC with a clear and consistent message on what the industry believes is the best and most efficient way to safeguard our markets. The Group, which represents a broad cross-section of the various types of market participants that filed comment letters on the NPR, discussed areas of commonality, as well as – and perhaps more importantly – where initial comments appeared to diverge.

In this letter, the Group provides its consensus opinion on how the Commission should implement regulation of electronic trading on designated contract markets ("DCMs") as well as addresses particular areas of concern with Reg AT that were discussed during the Roundtable with more granularity.

I. Overview on the Regulation of Automated Trading on DCMs

The Group offers the following overview on the regulation of electronic trading on DCMs. The principles outlined in this section offer a way for the Commission to move forward with regulation in this area. These principles cut across and inform the various issues discussed at the Roundtable. Accordingly, the Group provides the following recommendations as to what should be the focus of the Commission's Reg AT efforts.

---

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.

Since 1985, ISDA has worked to make the global derivatives markets safer and more efficient. Today, ISDA has over 850 member institutions from 67 countries. These members comprise a broad range of derivatives market participants, including corporations, investment managers, government and supranational entities, insurance companies, energy and commodities firms, and international and regional banks. In addition to market participants, members also include key components of the derivatives market infrastructure, such as exchanges, intermediaries, clearing houses and repositories, as well as law firms, accounting firms and other service providers. Information about ISDA and its activities is available on the Association's web site: www.isda.org.

SIFMA AMG's members represent U.S. asset management firms whose combined global assets under management exceed $34 trillion. The clients of SIFMA AMG member firms include, among others, tens of millions of individual investors, registered investment companies, endowments, public and private pension funds, UCITS and private funds such as hedge funds and private equity funds.

Broadly, across all components of proposed Reg AT, the Group believes that:

1. **Pre-trade risk controls** are the responsibility of all market participants, and when implemented properly and appropriate to the nature of the activity, have been proven to be the most effective safeguard for the markets, and should be applied comprehensively to **all** electronic orders.
2. Rules should not focus on any one specific type of market access, but, rather, should recognize the appropriate application of pre-trade risk controls to protect market integrity.
3. Regulation should **build on** and leverage the very successful risk controls and **safeguards currently in place** instead of proposing new and untested systems or procedures that would require significant investment by the industry.
4. Requirements **should not be one-size-fits-all**. Distinctions should be based on the business structure, business model, operational size, and technical sophistication of market participants.
5. **Rules should not be prescriptive**.

A. **Separate Consideration of Components of Reg AT.** There is wide agreement among the Group that the NPR tries to accomplish too much in one rulemaking and that the Commission and the industry would benefit from the separation of – as well as the opportunity to consider, comment on and hold roundtables on – different aspects of the rule. Indeed, we were pleased to hear Chairman Massad state that the Commission is open to implementing risk controls separately from other provisions of the NPR. The Group strongly believes that the Commission should focus on the implementation of appropriate risk controls in the first instance and subsequently address other important areas of the NPR in due course.

B. **Application of Reg AT.** The Group strongly believes – and history has shown – that any market participant, regardless of registration status or type of trader, has the potential to cause marketplace disruptions. A stated goal of the NPR is to mitigate such risks. The NPR, in its current form, falls short of adequately addressing this concern and, as a result, would leave the market exposed to potential disruptions that may be avoided or minimized by a rule with a more appropriate scope. All market participants have a responsibility appropriate to their participation in the life of an order to help minimize the likelihood of a market disruption, and, accordingly, all electronic trading should be subject to appropriate pre-trade risk controls. Such pre-trade risk controls can be implemented directly by the market participant or may be administered by the FCM facilitating electronic access to the market (and implemented within the appropriate system that the FCM has administrative control over, including third-party vendor systems and exchange provided graphical user interfaces).

C. **Definition of AT Person.** The Group also strongly believes that the proposed definition of AT Person fails to work with any of the major elements of Reg AT.[2] The CFTC seems intent on capturing a pre-determined number of market participants, and therefore identifying a metric to capture such traders, rather than focusing on the risks associated with all orders submitted electronically. After considerable discussion, the Group believes that instead of focusing on the definition of AT Person, the Commission should focus on all electronic orders being subject to pre-trade risk controls as discussed below.

(See Appendix 1 for additional details on the Group's position on Quantitative Measures raised during the Roundtable.)

D. **Registration.** The Group believes that if the CFTC is determined to implement a new registration requirement, then such registration should be considered separate and apart from the proposed pre-trade risk controls under Reg AT, and that such proposed registration category should be carefully defined.[3] Creating a registration category of AT Persons for the purpose of applying Reg AT confuses the issue and potentially encourages firms to simply adjust trading methods to avoid being in scope for registration without meaningfully reducing potential market disruption. If the Commission would start from the basic principle that all electronic orders should be subject to risk controls, the rule becomes much less complex to design and implement. The Group encourages the Commission to focus on what is truly important – implementing pre-trade risk controls to minimize disruption to the market – instead of imposing a poorly defined registration category with unintended consequences to market participants. Nonetheless, later in this comment letter we provide a potential alternative in the context of requiring the application of risk controls that may help the Commission meet its objectives.

E. **Risk Controls.** Rather than defining what constitutes an AT Person, and using an artificial trigger to require registration of those participants, we believe that the most important tool for achieving the goal of protecting market integrity is requiring the application of pre-trade risk controls to all electronic orders, regardless of the participant's registration status. The Group believes:

- **Each market participant's orders should be subject to pre-trade risk controls, depending on how the market participant accesses a DCM.** Access can be via self-developed software, a third party provided system or FCM-administered[4]

[2] The proposed definition of AT Person would require a narrow group of market participants to implement pre-trade and other risk controls whereas, we believe risk controls should apply to all electronic trading. At the same time, the proposed definition of AT Person would impose a host of unnecessary and burdensome documentation, reporting and testing costs and requirements under § 1.81 that not only would be inappropriately applied to all AT Persons, but certainly should not apply to a more broadly defined group of AT Persons.

[3] For the avoidance of doubt, market participants that are already registered with the CFTC should not be subject to any new obligation for additional registrations.

[4] It is important to note that a customer may use the same FCM to provide both execution and clearing services ("full-service FCM") or may use one FCM for execution ("executing FCM") and choose to clear their trades through

software and/or services. Orders from market participants leveraging FCM-administered systems, including those provided by third parties, may utilize pre-trade controls administered by the FCM.

It is important to note that the Group believes that market participants <u>not</u> using software that includes FCM-administered risk controls are responsible for applying risk controls to their own orders.

- **FCMs facilitating electronic access to a DCM should be responsible for implementing appropriate pre-trade risk controls for all electronic trading that passes through those controls that it administers.** This can be accomplished by pre-trade risk controls provided by the FCM itself, or those provided by software that the FCM has administrative control over.[5] Where a market participant is responsible for the administration of risk controls pursuant to Reg AT, the FCM may satisfy this responsibility by administering DCM hosted risk controls.
- **The risk controls proposed in the NPR are too prescriptive.** The specific implementation and location of particular risk controls should not be mandated by the CFTC. Instead, the types of controls required should be principles-based to provide for flexibility as well as to permit innovation and technological advances that could improve future controls. Accordingly, the required controls should meet the core principles of being designed to reasonably mitigate the potential for:
  a. Sending orders for too large a size to the DCM;
  b. Sending orders for a clearly erroneous price to the DCM; and
  c. Sending too many messages to the DCM.
- **Identical pre-trade risk controls need not be applied at all points in the order flow.** Pre-trade risk controls should not be duplicated in precisely the same manner across the order flow between market participants and DCMs. Pre-trade risk control requirements should permit flexibility such that the controls will be appropriate for their location and type of electronic access being provided, with varying degrees of sophistication and granularity depending on who is setting the controls.
- **The standard used to measure compliance should be that pre-trade risk controls *mitigate* the risks associated with electronic trading – rather than *prevent* them.**

(For a more detailed discussion of the critical role the FCM plays in setting risk controls today, see Appendix 2.)

---

another FCM ("clearing FCM") by arranging for the trades to be given up to the clearing FCM by the executing FCM. In this instance, the executing FCM acts as the "gatekeeper" to the DCM matching engine, and, as such, is the only FCM that can administer risk controls at a pre-trade level. Any other FCM(s) that may subsequently clear trades for the customer can only provide risk controls on a post-trade basis once the trades have been given in from the executing FCM.

[5] Note that administration of such controls may be delegated by the FCM to another party, such as an introducing broker.

F. **Access to Source Code.** The Group strongly believes that Source Code is critically important and sensitive proprietary information that demands the highest level of protection.[6] Accordingly, the Group believes that:

1. The Source Code requirement for unfettered access to a firm's intellectual property as proposed in the NPR is **unprecedented** among regulators and threatens commercially valuable intellectual property and proprietary trading strategies. We note that the federal government recently further acknowledged the importance of intellectual property by signing the Defend Trade Secrets Act into law in order to enhance protections against the misappropriation of intellectual property.
2. The Source Code requirement in the NPR puts highly proprietary information at risk **without measurable benefits**. Allowing regulatory requests for this code for any reason increases the likelihood of it becoming public, even if that is not the intent of the Source Code requirement. Such an incident would negate the value of any released source code, and create a significant loss to the Source Code designers and their customers.
3. Required production of Source Code should only be **available through a legal process** where an owner of Source Code has the right to petition a court for appropriate protection. There is no sufficient set of access conditions (*e.g.*, onsite review, tracking who reviews Source Code, etc.) that would adequately offset the dire potential commercial consequences of requiring production of Source Code absent the protection of legal process.
4. **Current practice** – which enables the CFTC or Department of Justice to seek a voluntary production of Source Code subject to agreed restrictions, or to request such Source Code via a validly issued subpoena in connection with a formal investigation – **is sufficient and should be continued**.

G. **Software Development, Testing, Deployment and Monitoring.** The Group believes that Reg AT's proposed rule 1.81 is overly prescriptive and is not properly crafted to take into account the multiple ways market participants may operate and administer algorithmic trading systems. Similarly, it does not adequately differentiate between algorithmic trading systems designed by a market participant and those designed and licensed by a third party, and indiscriminately imposes the same obligations on a market participant for both types of systems. In many cases, due to legally binding licensing agreements or organizational barriers, it would be impossible for market participants to satisfy the requirements set forth in proposed rule 1.81. Accordingly, the Group believes that:

[6] For this reason, some members of the Group are submitting a separate comment letter with the U.S. Chamber of Commerce and other industry representatives that solely addresses the NPR's treatment of Source Code. We present comments on Source Code in this letter to supplement those comments and present views specific to the derivatives industry.

1. Policies and procedures for the development, testing, deployment and monitoring of algorithmic trading (including third-party software) are not appropriately addressed in the NPR and need to be considered in a **separate rulemaking**.
2. The proposed rule does not take into consideration or address **unique issues** related to third-party software. Accordingly, the CFTC should not move forward on proposed rule 1.81 until the treatment of third-party software is addressed.

(See Appendix 3 for additional details on the Group's position on Software Development, Testing, Deployment and Monitoring of Third-Party Systems.)

H. **Self-Match Prevention.** The Group believes that the current DCM rules regarding self-trading in conjunction with DCM-provided self-trade prevention software are effective. The incidences of problematic self-trading are statistically insignificant and do not justify the creation of an entirely new, costly, and burdensome federal regulatory regime on self-trading.[7]

I. **Annual Reports.** Reg AT's proposed requirement of annual reports to be prepared by market participants and clearing member FCMs is ineffective, unnecessary, and redundant with other requirements to which registrants are subject. Additionally, the proposed reports will inundate DCMs with voluminous policies and procedures related to the development and compliance of algorithmic trading systems, as well as mountainous snapshots of stale quantitative risk parameter settings particularized to a given market participant that will be virtually impossible for a DCM to meaningfully assess.[7] Accordingly, the Group believes that the objectives of proposed Rule 1.83 can be met less onerously and more practically by requiring affected parties solely to **certify that they materially comply** with relevant aspects of the rule and to make such certifications available to a DCM or the CFTC upon request.

II. The Group's Response to Specific Issues Raised at the Roundtable

During the course of the Roundtable, Staff sought to elicit suggestions on how to better define DEA as well as proposals for quantitative measures to reduce the current population of AT Persons to which Reg AT would apply. In addition, the Staff questioned whether requiring and monitoring compliance by AT Persons could be imposed upon FCMs or DCMs. Roundtable participants soundly rejected these proposals, as they did not address the real issues and concerns on which the Commission and Reg AT should be focused. The Staff also sought input on the issue of Source Code. Accordingly, the Group provides the following recommendations as to what should be the focus of the Commission's Reg AT efforts.

A. Recommendations for Requiring the Application of Pre-Trade Risk Controls

As previously noted throughout this letter, the Group believes that all electronic trading should be subject to pre-trade and other risk controls appropriate to the nature of the activity. The Group believes that the FCM facilitating electronic access to the DCM through the

[7] See Initial Comment Letters for additional details.

FCM's infrastructure or software that is under the administrative control of the FCM is responsible for implementing the appropriate pre-trade risk controls.[8] Where a market participant's orders do not pass through risk controls administered by an FCM, the market participant has the responsibility to ensure appropriate pre-trade risk controls are in place.

(For a more detailed discussion of the critical role the FCM plays in setting risk controls today, see Appendix 2.)

Moreover, the Group strongly believes that registration status is not an appropriate trigger for determining to which market participants Reg AT should apply, or vice versa. Rather than define a registration category of AT Persons, we believe that the most important tool for achieving the goal of protecting market integrity is to require all electronic orders to have pre-trade risk controls, regardless of the participant's registration status. If the Commission nevertheless believes that it must tie registration to the application of these risk controls for fear that it cannot otherwise enforce regulation on non-registrants, we urge the Commission to consider the alternative framework below.

The Group's Recommendation for Registrant-Imposed Pre-Trade Risk Controls

The Group proposes a requirement that all electronic trading must pass through the pre-trade risk controls of a CFTC registrant – either the market participant itself, or the FCM that facilitates electronic access to the DCM. These controls are typically in addition to the risk controls provided at the DCM level. The details of this proposal are as follows:

- **SCOPE:** All electronic trading must be subject to pre-trade and other risk controls administered by a CFTC registrant that are appropriate to the nature of the activity. The responsibility for implementing the appropriate pre-trade risk controls lies either:
  a) with the FCM registrant that is facilitating electronic access to the DCM, or
  b) in the case of a market participant that is not trading through the risk controls of an FCM, with that participant, who is also a registrant.

  In both cases, these pre-trade risk controls must be supplemented by DCM-provided risk controls configured by the member of the DCO that grants access to the DCM.
- **REQUIRED PRE-TRADE RISK CONTROLS:** Required controls must meet the core principles of being designed to reasonably mitigate the potential for:
  1. Sending orders for too large a size to the DCM;
  2. Sending orders for a clearly erroneous price to the DCM; and
  3. Sending too many messages to the DCM.
- **IDENTIFICATION OF COVERED TRADES/PARTICIPANTS**: Market participants trading electronically, without passing through FCM-administered risk controls, either self-identify to applicable DCMs prior to trading, or may be identified via tags on order messages.

[8] See Footnote 4 above.

- **DUE DILIGENCE REQUIREMENT:** Consistent with existing general risk management requirements under CFTC Rule 1.11, an FCM must perform due diligence on any customer to which the FCM grants electronic access to the DCM without going through the FCM's administered risk controls, including with respect to the customer's pre-trade and post-trade risk controls. Such due diligence may include – for example – a self-certification by the market participant that their orders are subject to appropriate pre-trade and post-trade risk controls. For the avoidance of doubt, such due diligence requirements do not make the FCM responsible for ensuring their customers' compliance with their own regulatory obligations.

B. Recommendations for Retention of Source Code

There has been extensive discussion since the publication of the NPR on its Source Code provisions. For the reasons stated earlier in this letter and in our Initial Comment Letters, the Group does not support the requirement to provide Source Code to regulators outside of the subpoena process.

Notably, the discussion at the Roundtable seemed to focus on retention. The Group is supportive of a clearly defined, principles-based retention policy. Any requirement pertaining to maintaining and tracking changes to Source Code should be limited to our proposed definition for Source Code below. Those requirements should be principles-based, thus allowing organizations to select Source Code management tools that best meet their needs while satisfying the best practices described below. Any mandated, prescriptive Source Code retention requirement may require market participants to embark on an extremely complex and risky project to move existing Source Code repositories from one set of tools to another.[9]

The Group's Recommendations on Retention of Source Code

- **Definition of Source Code.** The first step in designing an appropriate retention policy is to define what is to be retained. Here the Commission should look to an objective standard that can be readily understood and applied by market participants. Accordingly, we propose that Source Code be defined[10] 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. Such discretion includes:

    1. The ability to submit, modify, or cancel the order.
    2. The ability to determine and set order details including:

[9] Such projects are rarely undertaken by software engineering organizations due to these well-known risks.

[10] Our proposed definition was derived from the Linux Information Project's definition of Source Code: http://www.linfo.org/source_code.html. We have modified that definition to take into account the context in which the definition is used within the NPR.

- 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 the order an order affecting request to the DCM

The definition of Source Code for the purposes of Reg 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).

- **Tracking Changes.** There are existing Industry **Best Practices** for maintaining and tracking changes to Source Code which could be incorporated into a retention requirement. Although the practice of maintaining and tracking changes to Source Code continuously evolves to meet the demands of the software engineering community, there are a few basic principles that have consistently applied to manage Source Code. They include:

  1. The owner of the Source Code should establish a repository[11] for that Source Code. This repository and its contents should be solely under the control of the owner of the Source Code. Multiple repositories may be appropriate depending on the organization's structure.
  2. Such repositories should include any version of Source Code that has been compiled into an executable system utilized for algorithmic trading in the production trading environment of a DCM. The Source Code representing an executable system utilized for production algorithmic trading should be retained for three years from the day of its last use for algorithmic trading on the production trading environment of a DCM.
  3. A process should be in place that enables auditing of changes to Source Code within the repository.
  4. A process should be in place that allows the owner of the Source Code to limit an individual's access to that Source Code as necessary.

Conclusion

The Group urges the CFTC to separate the rulemaking, focus on pre-trade risk controls and continue dialogue with the industry on remaining portions of Reg AT. The Group appreciates the opportunity to provide additional comment on this critical rulemaking and would welcome

[11] As mentioned at the Roundtable, the use of the term "repository" is not meant to imply that the Source Code will be sent to or stored by the CFTC or CFTC delegate.

the opportunity to continue to work with the Commission to provide further input during the final rulemaking process.

Respectfully submitted,

Walter L. Lukken
President and Chief Executive Officer
FIA

/s/ Stuart J. Kaswell

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

Katherine Tew Darras
General Counsel
ISDA

Laura Martin
Managing Director and Associate General Counsel
SIFMA AMG

Enclosures: Appendix 1, Appendix 2 and Appendix 3

cc: Honorable Timothy G. Massad, Chairman
Honorable Sharon Bowen, Commissioner
Honorable J. Christopher Giancarlo, Commissioner
Vincent A. McGonagle, Director, Division of Market Oversight
Sebastian Pujol Schott, Associate Director, Division of Market Oversight

Appendix 1

Response to CFTC Roundtable Questions on Quantitative Measures to Establish the Population of AT Persons

As highlighted by participants at the Roundtable, the Commission should not look to calibrate the scope of Reg AT based upon quantitative measures. Quantitative measures are generally ineffective because not only are they highly market specific, but they are also dependent on:

- the length of the observation period;
- the overall market activity during that period, and;
- the relative concentration or fragmentation of activity.

Moreover, quantitative measures would not properly identify the trading activity to which risk controls should be applied and raise a host of implementation challenges.

A quantitative measure would be an inappropriate tool to identify algorithmic trading activity and, in many cases, an unreliable indication of trading strategy. For example:

- **Trade Volumes**. Large-size transactions executed in the central limit order book are not an indication of an algorithmic trading strategy. In fact, a significant number of large transactions are attributable to manually submitted orders.
- **Trade Frequencies**. Aside from the frequency of order submission, a market participant does not have direct control as to the number of executions any single order would generate. Rather, the number of executions is dependent on the number of opposing orders the firm is matched against. For example, when a firm submits an order for 1,000 contracts, the trade may be filled in a single 1,000-lot execution or up to 1,000 separate one-lot executions. This trade frequency is not an accurate measure of trading strategy, as it only reflects the number of opposing orders in the market at any given time.
- **Order-to-Trade Ratios**. Although useful in promoting efficient markets, order-to-trade ratios are also an ineffective mechanism for identifying an algorithmic trading strategy as they serve primarily as a measure of the quality of quoting, and not an indication of strategy. Orders that are placed closer to the top of book are more likely to be filled and therefore result in lower Order-to-Trade Ratios. This ratio does not capture information that identifies the strategy employed by a firm other than that the prices included on the orders may ensure they receive a better fill ratio than another strategy.
- **Message Frequency**. DCMs have existing operational controls that establish message throttles to protect the orderly operation and integrity of the markets. Although messaging frequencies may correlate to the use of high-frequency messaging in some circumstances, they should not be confused with a singular definition of algorithmic trading as many algorithmic strategies do not result in high messaging counts. Passive, opportunistic, time and volume-based strategies may originate through algorithmic means, but would likely not result in a measured frequency or ratio that would identify algorithmic trading. Any definition that hinges on message frequency would certainly not be reliable enough to support a registration obligation.

In addition to being unreliable for purposes of identifying a trading method, quantitative measures are also difficult to implement. Such quantitative measures are likely to be only indicative of market conditions at the time of measurement and not specifically representative of algorithmic trading. A quantitative calculation is also highly dependent on it being applied by the appropriate entity, with the appropriate level of messaging information. For example, an FCM would not have full insight as to the overall messaging activity of a market participant because that participant's activity could potentially span across multiple FCMs.

Appendix 2

Response to CFTC Roundtable Questions on How Customers of FCMs Access Markets

A market participant may choose to access a DCM via several channels (please refer to Diagram 1 for examples). Many market participants may use a combination of channels to facilitate different types of trading, using tools that are appropriate to the type of activity that they engage in. With very few exceptions, an executing FCM facilitates electronic access for the customer, and administers pre-trade risk controls appropriate to the type of access.

1. In the context of electronic trading, an **Application Programming Interface (API)** is an interface for electronic access provided by one party for another party to connect directly without using a manual means of placing orders and receiving executions (see Graphical User Interface).

   Examples of APIs include the following –

   An API provided by a DCM for market participants to connect directly to the matching engine. Such APIs are usually proprietary to the DCM, and will offer functionality such as types of messages, order types, etc., that is specific to the DCM. Connection to the API is overseen by the DCM through a certification process. Subsequent to CFTC 1.73, the DCM provides pre-trade risk controls to the FCM that facilitates electronic access (see ❶ on attached diagram).

   The FCM administers pre-trade risk controls provided to them by the DCM, but greater responsibility lies with the market participant to implement their own pre-trade risk controls to mitigate the possibility of inadvertent market disruption.

   a) **An API provided by an FCM for market participants to connect via the FCM infrastructure**, with orders subsequently routed via the FCM's Automated Order Routing System (AORS) through to the DCM's API. Such APIs are usually based on the FIX Protocol, a global standard for the exchange of financial information across asset classes. An FCM's API may be used for routing orders directly from a customer's trading system or from a third-party trading system without using a manual means of placing orders and receiving executions (see Graphical User Interface).

      Pre-trade risk management for orders routed through an FCM's API is provided by the FCM before the order is subsequently routed to the DCM (see ❷❹ on attached diagram).

b) **An API provided by a third-party software provider for market participants to connect via their infrastructure**, with orders subsequently routed via the software provider's Automated Order Routing System (AORS) through to the DCM's API. Such APIs are usually based on the FIX Protocol, a global standard for the exchange of financial information across asset classes. A software provider API is used for routing orders directly from a customers' trading system or from a third-party trading system without using a manual means of placing orders and receiving executions (see Graphical User Interface).

Pre-trade risk management for orders routed through a software provider's API is provided in their system before the order is subsequently routed to the DCM (see ❸ on attached diagram). Such risk controls are typically administered by the FCM facilitating access to the DCM via the software provider.[12]

2. In the context of electronic trading, a **Graphical User Interface (GUI)** is an interface for access provided by one party for another party to manually place orders and visually receive executions.

Examples of GUIs include the following –

a) **A GUI provided by a DCM for market participants to place orders directly on the DCM**. Such GUIs are usually provided for functionality that is unique to the DCM and/or may not be readily available via the DCM API. In this situation, the DCM is acting as a software provider, and pre-trade risk management for orders entered though such a GUI is administered by the FCM facilitating access.

b) **A GUI provided by an FCM for market participants to place orders directly with the FCM**, with orders subsequently routed via the FCM's Automated Order Routing System (AORS) through to the DCM's API. Pre-trade risk management for orders routed through such a GUI is provided and administered by the FCM before the order is subsequently routed to the DCM (see ❷❹ on attached diagram).

c) **A GUI provided by a software provider for market participants to place orders directly via their infrastructure**, with orders subsequently routed via the vendor's Automated Order Routing System (AORS) through to the DCM's API. Pre-trade risk management for orders routed through such a GUI is provided by the software

[12] Note that where a non-FCM clearing member of a DCM uses a software provider to access the market, via either API or GUI, there is no second line of pre-trade risk control administered by an FCM. In such a situation where the non-FCM clearing member sets their own pre-trade risk controls, additional responsibility may be required on the market participant to ensure that all appropriate steps are taken to mitigate the possibility of inadvertent market disruption.

provider before the order is subsequently routed to the DCM (see ❸ on attached diagram). Such risk controls are typically administered by the FCM facilitating access to the DCM.

3. An **Automated Order Routing System (AORS)** is software designed to electronically route orders to a DCM, without any subsequent discretion in how to work the order. Any discretion regarding how to work an order based on parameters provided by a trader or customer - for example using algorithmic execution functionality - should be considered "algorithmic trading" and considered differently from an AORS.

   AORSs are utilized by many types of market participants, and typically offer pre-trade risk management functionality. It is important to understand ***who*** administers the pre-trade risk controls.

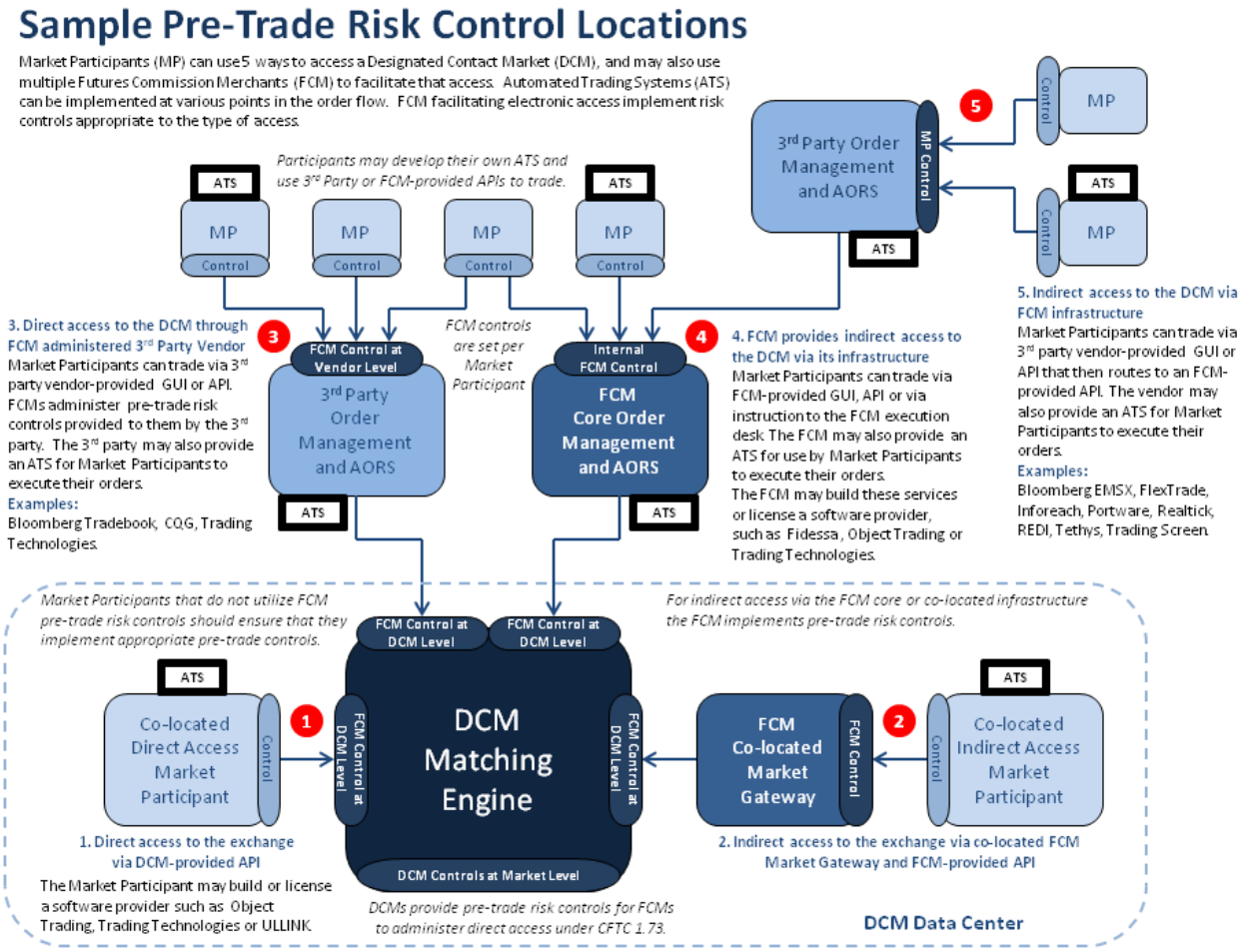
   Types of AORS include the following:

   a) **An AORS provided by an FCM where orders may be entered via an API or GUI and subsequently routed to the DCM's API** (see ❷❹ on attached diagram) using the FCM's membership on the DCM. Such a system may be developed in-house at the FCM or licensed from a third-party provider, but in either situation, the AORS is considered part of the FCM's infrastructure. Pre-trade risk controls are provided and administered by the FCM on a customer-by-customer basis. The FCM in this scenario is always the executing FCM, though they may also be the clearing FCM based on their customer relationship.

   b) **An AORS provided by a software provider where orders may be entered via an API or GUI and subsequently routed to the DCM's API** (see ❸ on attached diagram) using an FCM's membership on the DCM. The software provider gives FCMs the ability to permission the customer to trade and set the appropriate risk limits. Although such a system is not fully under the control of an FCM, especially where the AORS provides access to multiple FCMs, it can still be considered an extension of the FCM's infrastructure because a customer may not trade until the FCM sets appropriate pre-trade risk controls. As such, pre-trade risk controls are administered by the FCM on a customer-by-customer basis. The FCM in this scenario is always the executing FCM, though they may also be the clearing FCM based on their customer relationship.

An AORS utilized by a market participant where orders may be entered via an API or GUI and subsequently routed to the DCM's API (see ❶ on attached diagram). Such a system may be developed in-house by the market participant or licensed from a software provider, but in either case is considered part of the participant's infrastructure. Pre-trade risk controls are

administered directly by the participant, and not by an FCM. The AORS is certified by the DCM to connect directly to its API, and access is facilitated by an FCM via its membership on the DCM . The FCM in this scenario is always the executing FCM, though they may also be the clearing FCM based on their customer relationship.



Appendix 3

Response to CFTC Roundtable Questions on AT Persons' Compliance with Elements of the Proposed Rules when Using Third-Party Algorithms or Systems

FIA believes that it will be very difficult for a market participant to adhere to the requirements for development and testing, regulatory compliance, and documentation as proposed in § 1.81 of the NPR due to their overly prescriptive nature. These requirements become all but impossible to implement when using third-party software. In addition to the concerns with the development, testing, compliance and documentation requirements of proposed § 1.81 as raised in the Initial Comment Letters on Reg AT, the Group specifically highlights the following issues posed by the use of third-party systems:

- **Maintaining a development environment separate from the trading environment**. This separation would necessarily be the case because a third party is performing development and is not operating the trading platform. However, the customer of a third-party system would have no control over how such an environment is operated or configured.
- **Testing of all algorithmic trading code and related systems and any changes to such code and systems prior to implementation**. While it is best practice to test the algorithm developed within a third-party system, it would not be possible to test the entirety of the third-party system to the extent described in rule 1.81. More importantly, a customer cannot stipulate that such testing be documented in a certain way. A vendor may provide service level agreements guaranteeing a certain level of testing, but the customer would have no knowledge as to whether such testing took place and would only be able to gain monetary compensation should it become evident that testing was not done according to the agreement.
- **Regular back-testing of algorithmic trading systems using historical transaction, order, and message data**. Although the customer may be able to operate the third-party software in such a way as to back-test for the circumstances that may contribute to future Algorithmic Trading Events, the customer would have little ability to pinpoint what is causing the issues that contribute to such events and would have to rely on the vendor to correctly mitigate and remedy the issue. This would be extremely inefficient and time-consuming.
- **Regular stress tests of algorithmic trading systems to verify their ability to operate in the manner intended under a variety of conditions**. As with back-testing, this requirement is problematic for the customer. Although the customer can perform a stress test while operating the algorithmic trading system, it would not be able to identify the source of the issues that may arise and it would have to rely on the vendor to identify and remedy this issue. This would not be conducive to efficient testing of the algorithmic

trading system and would place an inappropriate burden on the customer who is operating such system.

- **Procedures for documenting the strategy and design of algorithmic trading software used by a market participant as well as changes to such software if such changes are implemented in a production environment**. The customer of a third-party vendor would have no ability to document the strategy, design, or changes made to a third-party system. Indeed, the third-party vendor would be unlikely to make available documentation of any of these actions due to protection of intellectual property. The market participant may be able to document its strategy for operating the third-party system, but it would be unable to produce sufficient documentation as to how the algorithm was in fact designed or whether the strategy was properly designed to conform to the intention.
- **Maintaining a Source Code repository to manage Source Code access, persistence, copies of all code used in the production environment and changes to the code**. Due to intellectual property protection, a third-party vendor would be unlikely to give access to Source Code to its customer and unlikely to take direction from a single customer on how the Source Code is stored and what changes are made by whom.

As is clear from the discussion above, a market participant would be able to confirm only that its operation of a third-party algorithmic trading system is tested and documented. It would have little to no control over how the third-party system itself is developed, tested, stored, or configured. Nor would the market participant be able to provide access to a regulator to information of how the third-party system was designed or tested. Accordingly, a market participant would be unable to meet the requirements of proposed § 1.81 for any third-party algorithmic trading system it is operating.

It is important to note that if the requirements for developing, testing, deploying and monitoring of self-developed algorithmic trading systems remain overly prescriptive while the requirements for third-party systems become more operational, market participants will have an incentive to use third-party systems in lieu of self-developed software, which may lead to a condition where the Commission has less control over the risks of algorithmic trading system development.