



CFTC ROUNDTABLE ON REGULATION AUTOMATED TRADING

OVERVIEW

For questions please contact [Kwon Park](#) at (202) 547-3035.

Today, the Commodity Futures Trading Commission's (CFTC or Commission) Division of Market Oversight (DMO) held a [roundtable](#) to discuss proposed Regulation Automated Trading (Reg AT).

Key Takeaways

- In the first and third panels, DCMs and FCMs disagreed as to whether risk controls should be maintained at the DCM or FCM level, while some of the panelists indicated that risk controls should be provided at the point where an order meets the DCMs matching engine.
- In the first panel, all of the panelists agreed that the definition of DEA captured too many market participants and that the definition should be revisited.
- In the second panel, all panelists expressed concerns on using quantitative metrics to establish the population of AT Persons.
- In the last panel, panelists stated that source code is proprietary and the intellectual property (IP) of trading firms. With the exception of one panelist, everyone asked the Commission to maintain its current process of utilizing a subpoena when requesting a firm's source code.
- With regard to source code, Chairman Massad said that the CFTC understands source code to be proprietary and of significant value to firms, and that the Commission will do everything to find the proper way to obtain access moving forward.

SUMMARY

Opening Statements

Chairman Timothy Massad

- The Commission is open to constructive and practical ideas, and will decide on the process of this rulemaking after this roundtable.

[Commissioner Sharon Bowen](#)

- A number of observers have raised questions about certain granular elements of our rule, including how to deal with source code and the role of third party service providers – hope this roundtable shows that the Commission is sensitive to stakeholders' concerns about this rule.
- Time is of the essence when it comes to regulating automated trading, and I take to the concerns of end-users very seriously. For end-users to express such concern about algorithmic (algo) trading gave me pause. While I believe algo trading has brought some benefits to our markets, it is clear that some of our key market participants have serious concerns about it.
- I hope to finish a strong and effective regulation on automated trading this year.

Commissioner Christopher Giancarlo

- The proposal's seemingly broad scope, hazy objectives, and several significant inconsistencies are problematic. Its burdensome and overlapping compliance costs will serve as a regressive tax on market activity, be borne disproportionately by smaller market participants, and be passed on to end-users.
- The source code requirement that it be accessible to the CFTC and the Department of Justice (DOJ) without a subpoena has brought enormous concerns. Proprietary source code for future strategies are not equivalent to books and records.
- Compared to the brashness of its dispensation with subpoena authority, Reg AT's most notable feature is the meagerness of its response to the emerging challenges of algo trading. In essence, Reg AT is a 20th century analog response to the 21st century digital revolution in trading markets.

Amendments to the Definition of Direct Electronic Access (DEA)

Joseph Otchin, DMO: The Commission is considering three alternatives: 1) using the proposed definition of DEA; 2) using the definition in CFTC regulation 38.607; or 3) revising the proposed definition – thoughts? **Jim Moran, CME:** The definition should be altered as “an arrangement where a person electronically transmits an order to a DCM without the order first passing through a risk control administered by a DCO under revised 1.82.” This definition focuses on what is most important - whether important pre-trade risk controls have been applied by the clearing member. This definition also deals with third party software users.

Sebastian Pujol Schott, DMO: How would the population of captured participants change in this alternative definition? **Moran:** The Commission should distinguish between financial versus algo risk controls. The current proposal is abundant and risk controls at every level is too granular. Risk controls should be at the clearing firm level because there are clearing firms that are not FCMs. DCMs have lots of controls, but the focus should be on the point of execution. DCMs have certain controls on all orders (i.e. price banding, etc.) and are not set based on each participant, but applies to everyone equally; **Douglas Carucci, JP Morgan:** It is hard to understand how a clearing FCM has the ability to interrupt bad orders or to put controls around trading activity in real-time. The DCM is the last line of defense, as it holds the matching engine. The bulk of responsibility should be at the DCM. Moving away from the DCM, the person who develops and operates applications with a DCM interface should have the next layer of defense; **Gregory Wood, Deutsche Bank:** Risk controls should be in place for members accessing DCMs. Clearing FCMs do not always execute on behalf of the client. The DEA definition, as proposed, is too broad and should not capture those using third party software (i.e. order routing systems). The risk controls should lie where the FCM provides access to the market. Before providing access to the market, FCMs perform adequate qualitative and quantitative checks on its customers; **Nitin Gambhir, TT:** This regulation is impossible to manage and captures too many entities. The party submitting orders to the DCM is where risk controls should be provided. The Commission should focus on defining “risks” and allow market participants to build controls around the risk definitions.

Otchin: How can the Commission narrow the definition? **Gambhir:** DEA should be where a firm can generate an order, and execute at the DCM matching engine directly.

Schott: What layers of controls are calibrated at the DCM level? **Moran:** The DCM does not provide risk controls at a granular level, the FCM knows its customers better and can better manage different level

of controls in a meaningful way; **Kurt Windeler, ICE:** The proposal uses DEA as a filtering mechanism to register firms. FCMs know their clients and can set risk controls to their preferences. DCMs apply certain risk controls that apply uniformly to everyone.

Schott: How can risk controls be designed, calibrated, and controlled by someone other than the trading firm? **Gambhir:** DCMs have order level information but it is unrealistic for DCMs to set parameters on trading firms – the FCM knows its customers best; **Carucci:** Before an order hits the matching engine, there is no doubt the DCM knows how that order will impact the market and that it is the last line of defense; **Jeff Burnett, QIM:** FCMs already have controls; **Venu Paleparthi, Virtu Financial:** Having direct access to markets comes with certain responsibilities, and registration is one. Exchanges are not in the position to know trading strategies, but can implement controls as an ultimate backstop to preserve market integrity. FCMs serve the financial risk mitigation function.

Otchin: What market participants does 38.607 capture? **Moran and Windeler:** 38.607 captures almost every market participant and is much broader than proposed DEA; **Waseem Baraei, One Chicago LLC:** Both definitions would capture the same type of activity and the same type of market participants.

Quantitative Measures to Establish the Population of AT Persons

Alberto Garcia, ESMA

- Garcia provided an overview of MiFID II and how the Europeans used quantitative metrics to identify algo trading, high frequency trading (HFT) firms, and investment firms. He explained how the Europeans identified firms in these categories by using two metrics provided by the Germans and the French. He also explained that algo trading and HFT firms were subject to different requirements.

Michael Penick, DMO

- Staff is considering balancing the number of firms captured under the AT Person definition by using quantitative thresholds in the DEA definition. Staff is considering thresholds on, for example, order resting time, trade counts, trade volume, and etc. DMO solicits comments on the benefits and challenges of harmonization with Europe.

Richard Hayes, DMO: If the Commission chooses to introduce a quantitative metric, are there certain metrics that are most appropriate? **Adam Nunes, Hudson River Trading:** There is no difference in the risks posed to the market for firms trading high versus low volumes. The Commission should not focus on measures that consider trading strategies as it may exclude others that pose the same risks.

Giancarlo: If risk controls are mandated based on certain thresholds, would firms adjust strategies to stay below the threshold? **Nunes:** Depends on the circumstances; **Carl Coscia, Hartree Partners:** The Commission should not implement a rule that hampers innovation. Speed is not the enemy. The focus should be on how quickly an order can be disengaged and on other risk metrics; **Matthew Picardi, Shell Energy on behalf of CEWG:** Risk is better managed by FCMs and DCMs. We do not have the market information to determine a good metric; **Isaac Chang, AQR on behalf of MFA:** Metrics depend on who the regulation is trying to capture (risk controls and registration). Hard thresholds are difficult to compare across products and difficult to calibrate accurately. Any metric is difficult to apply because market making and high frequency algos have a high concentration ratio, and is essentially a tax on

cancelled orders which will have an unintended effect of widening spreads and reducing liquidity. It is difficult to apply a one-size-fits-all metric to the marketplace; **Windeler**: Quantitative measures only identify strategies and not the risk of market disruption. Order ratios, trade frequency, etc. are not related to algo trading. Metrics will become a registration process for market makers and does not implement protections for people engaging algo trading.

Bowen: Are there specific market behaviors that introduces more risk? **Chang**: Risk should be divided into buckets: market based risk, operational risk, intended behavior, and unintended behavior; **Nunes**: Credit and financial risk are the most fundamental risks and easy to quantify, and already solved. The ability to stop orders before it hits the matching engine (i.e. message throttles) will help limit operational risk; **Burnett**: The Commission must strike the right balance to capture risks and not limit how people transact in the marketplace; **Koeling**: It is important to figure out who needs to be registered and where the risk controls should be placed. Risk controls should be implemented for every order. FCMs know-your-customer (KYC) position is a good model in figuring out where risk controls should sit and who should manage them – risk controls should be principles based. Optiver has many controls in place for our own protection. When there is a change to strategy, it is when things are more prone to go wrong, as opposed to a system that has been in place and proven to work; **John Mueller, KCG**: Single orders can cause market disruption. The focus should be where the control lies and who manages and develops those controls.

Hayes: What are certain risk control requirements or thresholds that are not appropriate? **Coscia**: Setting the lowest common denominator can discourage innovation and diminish liquidity. Any metric the Commission sets will be outdated for current market conditions; **Windeler**: Metrics are fully conditional on markets and market conditions. Any sort of frequency or relative measure as to messaging activity does not represent potential risk to the marketplace.

Alternative to Imposing Direct CFTC Pre-Trade Risk Control and Development, Testing, and Monitoring Standards on AT Persons

Alberto Garcia, ESMA

- Garcia said that in Europe, ESMA requirements, approved in 2015 and subject to a vote by the Commission in upcoming days, sets risk controls at two levels, the firm level and the DEA provider. He explained these firms would be subject to annual reports, pre-trade risk controls, KYC requirements, among others. Also, he said trading venues will have to set their own controls as a line of defense.

Marilee Dahlman, DMO: Discuss whether FCMs can require risk control requirements on its customers and whether it can perform due diligence on their customers, **Wood**: FCMs have KYC requirements in place. The focus should be on customers who want to access the markets and less about their trading strategies; **Matthew Lisle, ABN Clearing**: FCMs have KYC procedures and risk limit procedures – current regulation 1.73 works. Compliance in carrying out the proposed framework will cost us about \$1 million per year as a small FCM. The Commission already has the tools in its rules and regulations to set controls. The status quo is working; **Andres Choussy, JP Morgan**: Requiring FCMs to monitor client risk controls is only possible if we have our staff within that organization permanently to perform due diligence. Each client is significantly different and an FCM would need to account for that when setting controls.

Schott: If an FCM has a DEA client in Europe, what are anticipated staffing requirements? **Choussy:** As high as one employee per client; **Paleparthi:** FCMs should do their KYC and let us operate. We already have sufficient risk controls in place.

Dahlman: How can FCMs evaluate the adequacy of a clients systems and controls, and what criteria should be used? Any areas FCMs can conduct due diligence to control algo trading risk? **Lisle:** Look at execution risk controls. However, it is difficult to evaluate algo development. Anything in the trading environment will be relative to activity; **Wood:** Not all clients are engaged in algo trading. Regardless of access, we need principles based requirements. FCMs accept they have responsibility and 1.82 provides a good template for risk controls at the executing FCM level. However, it is difficult trying to perform due diligence on particular clients; **Choussy:** Look at the number of markets, products traded, means of trading, venues utilized, capital of each firm, and available resources; **Nunes:** FCMs do not want to be subject to these requirements and their clients do not want the FCM doing this. The NFA should review risk controls and perform due diligence.

Schott: Any benefit in giving a greater role to DCMs? **Barazi:** We prefer the DCM approach versus the FCM approach. DCMs are better able to review AT Persons and low latency firms; **Moran:** Making DCMs supervise AT Persons does not make sense; **Wood:** How AT Person is defined impacts the overall rule and will determine who should be responsible to oversee the AT Person; **Coscia:** Floor trader registration is outside of the Commission's policy and objectives.

AT Persons' Compliance with Elements of the Proposed Rules when Using Third-Party Algorithms or Systems

Drew Shields, TT: As a third party provider, we do not provide customers with access to source code. The question is whether our clients have a means to test our algos before using it.

Chang: AQR uses both internal and external algos to execute orders, and works with third party providers to test algos. The standard of care should not vary for those who develop algos versus those sold or leased by third parties. Everyone should be subject to the same requirements.

Gambhir: Clients can test in real time and historically how their algo performs. It is up to the client to manage risk layers and to prevent unintended incidents.

Mark Schlegel, DMO: Is testing required on algos, and if so, do firms record those results? **Shields:** We work with clients to meet regulatory requirements, but simply provide tools to access the markets for those without capital to connect directly. All test cases are documented for our own internal tests, but we do not record client tests.

Schlegel: Do clients ask third parties to create and design systems comply with rules? **Gambhir:** We perform due diligence; **Shields:** We do not make contractual representations but we do go over how and what test we performed with clients. We constantly modify and adjust to changing regulatory requirements. There should be no obligation for third party providers to certify any services and any additional tests should be up to the AT Person; **Picardi:** Making our firm register as a floor trader would make us (a commercial end-user) a financial entity subjecting us to margin and other requirements; **Lisle:** The responsibilities should ultimately be at the registrant level, whether you use a third party system or not.

Schlegel: Should Reg AT require a certification and due diligence framework for third party technology? **Gambhir:** Everything depends on how AT Person is defined; **Shields:** Just because a client did not write the code, does not mean they cannot comply. Customers should be able to test the algo without a certification from a third party provider. They can choose to use or refrain from using our services.

Schlegel: Can regulators request third party providers' source code? **Shields:** We provide and have provided the CFTC access to observe certain aspects of our source code through the subpoena process. Source code is the IP and lifeblood of our firm.

Source Code Access and Retention

Carlin Metzger, DMO: What do panel participants or commenters suggest as an appropriate definition of "source code" consistent with the intent of proposed § 1.81? **Mueller:** The execution path of an order, how the order was created, the decision to create, modify or cancel that order. Our source code is not a normal books and record and requires a higher thought process crucial to firms that develop the code. Classifying parameters around source code is challenging. Internal log files contain some information provided to the exchange, but a line has to be drawn as particular information in the log files may contain sensitive information; **Koeling:** Our internal log files contain massive amounts of information and every change in the source code is logged. These big log files are not kept for long periods of time and are used for our own debugging. We do not want log files in the public, as this might contain part of the source code.

Metzger: What software or hardware components should be included within the term "Algorithmic Trading System" to help ensure that appropriate systems are subject, for example, to the development, testing, and other standards in proposed § 1.81? **Mueller:** As a general practice, everything is tested before going into the production environment.

Metzger: To the extent that a panel participant utilizes hardware such as a Field Programmable Gate Array (FPGA) or an Application-Specific Integrated Circuit (ASIC), please describe the files or records used to create the hardware design to be placed on the FPGA or ASIC chip? **Mueller:** Internally, we maintain strong controls, and have ring-fences around the organization on who can access and see certain types of the source code; **Chang:** All the changes to the software system are logged and when a bug is found it is backed out. MFA as a whole believes the costs of recordkeeping must be balanced with the benefit of maintaining the files for a long period of time.

Schott: Assuming a circumstance where the Commission must review or inspect algorithmic trading source code, what options do panel participants or commenters suggest for review or inspection of such algorithmic trading source code? **Chang:** I agree with Chairman Massad's February Congressional testimony that a subpoena to access source code is a reasonable standard. Source code contains trading instructions and is highly sensitive IP that drives the actual trading execution. Source code should not leave the firm's premises if regulators must see it. There should be some measure of due process and a burden of proof to protect the IP in question; **Shields:** Source code has been requested twice in my time at TT by the CFTC through the subpoena process. There was a review on-site, no copying of the code, and information was logged (who saw what and when). Regulatory bodies were able to see what they needed to further their investigations within this process. The subpoena process works and will continue to work.

Massad: Whether requested with a subpoena or not, the CFTC takes this seriously and understands source code is proprietary and of significant value to firms. We will not take this lightly and will do everything we can to protect confidentiality and the proper way to obtain access moving forward.

Marcus Stanley, Americans for Financial Reform: Source code is a set of trading instructions and should be a part of books and records. The government has a history of handling sensitive information (i.e. bank stress test models).

Please let us know if you have any questions.

Best,

Kwon Y. Park