TESTIMONY
OF
MICHAEL G. RYAN
EXECUTIVE VICE PRESIDENT AND GENERAL COUNSEL
TRADING TECHNOLOGIES INTERNATIONAL, INC.
BEFORE THE

House Agriculture Committee Hearing
Examining the CFTC's Proposed Rule: Regulation Automated Trading
July 13, 2016

Good morning Chairman Conaway, Ranking Member Peterson and members of the committee. My name is Mike Ryan and I am Executive Vice President and General Counsel at Trading Technologies International, Inc. ("TT"). TT is an independent software vendor ("ISV") of approximately 400 employees, we are headquartered in Chicago and have offices in most major financial centers throughout the world. TT licenses software trading solutions enabling its customers that include the largest banks, commercial firms, hedge funds, proprietary trading firms and other professional traders to trade on 45 of the world's major electronic exchanges and liquidity platforms. TT's electronic trading solutions, which are either housed at our customers' facilities or hosted by TT in co-location facilities, enable TT customers to trade using several automated trading tools, pointing and clicking on a market, or by inputting and utilizing their own proprietary algorithms to trade on electronic exchanges.

Most exchange-traded derivatives are now traded electronically, and electronic systems that connect to exchanges, as well as algorithmic trading, have introduced new risks to markets that were not present in open-outcry environments. The daily increasing enhancements in processing and connection technologies including housing trading strategies on servers that are co-located with exchange matching engines constantly accelerates the speed of trading to new levels and amplifies these risks.

I am proud that TT has historically been in the forefront of helping the exchange-traded derivatives industry manage risks associated with electronic trading, by offering trading systems that include comprehensive risk-management features that can be administered by customers, but ultimately controlled by their futures commission merchants—who provide the gateway to derivatives exchanges.

As an ISV, I believe that TT provides a perspective on some of the issues relating to the proposed Regulation Automated Trading ("Regulation AT") that is different than many of the other market participants represented here today. In that regard, I appreciate the opportunity to testify before you and I hope that my testimony will help the committee understand some practical aspects of the regulation and how it might be implemented using technology in place today.

We have raised some concerns about Regulation AT in other formats, including through public comment letters[1] and today I would like to testify on the following three aspects of Regulation AT:

1) The definition of "Direct Electronic Access" ("DEA");
2) The need for and propriety of a source code repository; and
3) The testing requirements relating to algorithmic trading applications.

[1] See attached Comment letters dated March 15, 2016 and June 24, 2016.

1) Definition of “Direct Electronic Access”

TT believes that the definition of DEA in Regulation AT should be clarified to indicate that there is no DEA where the orders are routed to a Designated Contract Market through the trading/order routing system of a member of a derivatives clearing organization (“clearing house” or “DCO”) where the pre-trade and other risk controls are able ultimately to be controlled by such member, including when a third party maintains the physical location of the systems.

As drafted, Regulation AT defines DEA as an arrangement where a person electronically transmits an order to an exchange without the order first being “routed through a separate person” who is a member of a clearinghouse to which the exchange submits transactions for clearing. As proposed, any non-CFTC registered person engaging in the trading of futures or swaps through DEA would be required to register with the CFTC as a “Floor Trader” and be subject to a host of prescriptive requirements – as would all persons designated as “AT Persons” under the contemplated CFTC rules.

However the proposed definition of DEA is unclear as it does not provide sufficient guidance as to what “being routed through a separate person” means. The definition of DEA, as drafted, may suggest that the order would also have to be routed through a system physically controlled by the DCO member, but such physical control really has nothing to do with actual control of risk management or the goal of enhancing risk management of such orders. The ultimate ability to exclusively control risk parameters is the relevant issue and that is typically achieved remotely using software applications. For example, using TT systems, a risk administrator is able to sit at his or her desk in Chicago and set risk parameters for traders who may be physically located anywhere in the world.

One suggestion for modifying the definition would be to add “(including through a system physically managed by a third party retained by such member to act on its behalf)” after the phrase “who is a member of a derivatives clearing organization.” Such clarification would not diminish any DCO member’s ability to control risk, would reflect the manner by which such risk is often administered today and the legitimate goal of the new regulation would still be achieved.

Without clarifying the language, the definition of DEA will likely capture within the definition of “Floor Trader” many single traders, small trading groups and even larger companies like energy firms and agricultural Co-ops and merchants who hedge on futures exchanges, all of whom trade through DCO members and are often substantial liquidity providers. The prescriptive requirements imposed on Floor Traders will add layers of administrative complexity to their businesses and require them to hire expensive compliance experts to their staffs. Yet, no further risk oversight would be achieved because a DCO member’s oversight is already fully integrated into the available trading systems.

2) Source Code Repository and CFTC/Department of Justice Inspection Authority

Proposed CFTC Regulation AT also requires AT Persons to “maintain a source code repository to manage source code access, persistence, copies of all code used in the production environment, and changes to such code.” Source code in a repository would be subject to the inspection by both the CFTC and the Department of Justice (“DOJ”) without subpoena or any formal opportunity by a source code owner to object or endeavor to restrict the manner of access or use of the source code.

Like many in the industry and at least one CFTC Commissioner, TT believes these requirements and the CFTC and DOJ's inspection authority are unnecessarily and extraordinarily broad, not likely to provide helpful information, likely constitutes an unconstitutional taking of individuals' property and is generally unnecessary to achieve the goal of the proposed regulations. TT recognizes that subsequent to the publishing of Regulation AT, the CFTC indicated publicly that it did not intend for the source code "repository" to be held by the Commission, but TT's concerns remain.

a. Source code is highly proprietary and typically not made available to third parties

Except with respect to open source licensing arrangements, to my knowledge source code is never licensed under any software license agreement offered by any software provider including any ISV in the futures or securities industries or any software firm such as Microsoft or Google. The source code of any trading firm or technology firm goes to the essence of the value of such companies. It is highly proprietary, trade secret information that could expose the fundamental aspects of a business that provide economic advantage over competitors. Making such valuable intellectual property readily available to the Commission is unnecessary to fulfill the intent of the regulations. The CFTC is no less prone to potential cybersecurity attacks than other government agencies and private companies, and two recently well-publicized instances provide real life examples of why firms would be gravely reluctant to turn over their proprietary source code to the CFTC or any government agency except under the highest level of protections. In each of these cases ex-government regulators– one from the New York Federal Reserve Bank and the other from the Food and Drug Administration–obtained and shared confidential information from their ex-government employers with their then current private employers.

b. Source code is complicated and the potentially relevant amount of source code is enormous

Frankly, it is doubtful that source code would readily be useful to the Commission. One engineer's source code is rarely drafted in the same manner as another engineer's and without proper documentation to help decipher the code it is often meaningless. Even with proper documentation it would often take insight from multiple engineers to decipher the intent of the code and documentation.

The breadth of the relevant code might also be so expansive that it is hard to fathom how it would be compiled, stored or used effectively. Each layer of code is very relevant to how an algorithm might function. Additionally, any number of different coding languages might be used in each application and at each layer of software. TT, alone, uses over 30 different coding languages.

A useful example of the underlying complexity of seemingly simple commands appears in TT's first comment letter to the Commission.

i. Market data adds another level of complexity

Similarly, without the exact same market data flowing through it, the myriad software applications interacting together may not work the same. Replicating the market data is likely a bigger problem than it seems because trading programs often coalesce data. Moreover, how and when coalescing occurs may vary from moment to moment depending on many factors such as network routers, firewalls, switches, server hardware, operating systems and vendor software.

Multiplying the complexity exponentially, the Commission would likely have to replicate market data at a particular moment from multiple markets, because trading algorithms will typically use and analyze data from many related markets, for example, equities and/or stock options if trading stock index futures. So, even if the Commission could recreate the prices in a market precisely as they were disseminated by the exchanges or other relevant markets, the software would likely act differently on different occasions despite using the same market data.

c. Making source code readily available to regulators would not reduce the risks

Even assuming, for the sake of argument, that the Commission could decipher the morass of relevant source code and the complexities of dealing with market data, there is no compelling need to gain access to the code because it adds very little to reduce the risks of algorithmic trading.

The outcome of the trades are indisputable evidence of the actual outcome of an algorithm and are already available in the form of the trade data (orders, fills, quotes sent to and matched at each exchange). Unusual results and/or repeated outcomes demonstrate the intent of traders and usually no more is necessary to establish intent.

The published guidance from exchanges and the CFTC regarding market manipulation cases recognizes that the culpability of a trader depends upon the conduct of the trader over time. Single trades rarely, if ever, give rise to the sort of culpability that would trigger a market manipulation case. Rather it is a series of events and a pattern of activity that might indicate a trader's intent or whatever the level of culpability is required to prosecute a case. Similarly, the code of an algorithm rarely if ever would prove the sort of culpability necessary to prove a market manipulation case. Many perfectly legitimate algorithms that are typically used to advance innocent trading strategies might also be used nefariously by bad actors. For example, TT and, I believe, all ISVs in the futures industry have functionality in their trading systems that would stop a trader from executing a trade with himself. TT's unimaginative name for this feature is "avoid orders that cross." Trading with oneself is prohibited on most exchanges, so this sort of functionality is mandatory for most of TT's customers. However, I understand that some alleged bad actors may have utilized this functionality to manipulate markets. The alleged facts in these cases are that a large order is entered on one side of the market and then another entered to cross the first order. The first order would be pulled from the market and the second order would be entered. In this scenario, the alleged bad actor would have used an otherwise perfectly legitimate trading tool to move the market toward the first order, which was never intended to be filled. The functionality (i.e., algorithm) would not be helpful to prove manipulation in this case because, as mentioned above, there is a perfectly legitimate use for the functionality. Rather, only the alleged bad actor's behavior over time could establish culpability.

Even in the unlikely scenario where the code of an algorithm might be helpful, the subpoena power of the Commission would be more than adequate to insure that the code is reviewed when truly necessary, although we continue to question when that would ever be the case. In fact, subpoenaing a written description of the intent of a trade or the basic algorithm that describes the strategy should be sufficient for most regulatory purposes. For example, a basic algorithm might be described as simply as “if market price = X then enter buy order at Y.” Such a simple description indicates the purpose of the algorithm much more clearly and easily than the vast expanse of source code that might otherwise be required under Regulation AT.

It is worth noting that over the 17 years that I have worked at TT we have been contacted regularly by exchanges and governmental agencies like the CFTC and DOJ who are investigating trading manipulation and other cases. We are fortunate enough to have a large customer base that depends upon TT software every day for their livelihood. Unfortunately sometimes our customers are accused of violating regulations or rules while trading with TT software. As a result, we are asked to help the exchanges and government agencies understand how TT software works so that they can better understand what a trader may have been doing. We always cooperate to the extent possible by providing verbal descriptions, written documentation and tutorials where appropriate. We also receive subpoenas relating to these cases and, of course, comply by producing information as required. Interestingly, despite such regular interaction, we have never once been required to produce the source code of any of our products. I believe this is the case because source code is not a necessary or desirable piece of evidence that might be used to avoid market disruption or prove or disprove bad acts in the marketplace.

3) Section 1.81 testing requirements should be limited to testing finished products

The last issue that I want to address is the testing requirements set forth in Regulation AT. TT believes that such testing should focus on the output of an Algorithmic Trading system or software rather than the source code underlying such systems or software, which would yield no material benefit.

As proposed, source code underlying an Algorithmic Trading system would be subject to substantial, highly prescriptive testing in advance of a system’s roll-out and continually afterwards.

a. Only testing of the finished product is relevant to Regulation AT

Any software product provided by TT to any customer is always tested internally by TT and is also available for the customer's testing. TT expects that each customer performs appropriate testing prior to utilizing the software in production environments, especially when the product is an algorithm that might be used for trading. In fact, TT offers testing environments that simulate market conditions to facilitate such testing. Such functional testing of a product is conducted to determine whether the output is consistent with the intended purpose of the product. The intended purpose is typically described in documentation provided by TT or any other developer of the product.

An important distinction between the sort of testing that clients perform every day on their software products and the proposed language of Regulation AT seems to be that the proposed rules require a registered entity to test software code (see, 1.81(a) (ii)) as opposed to the finished product that the entity developed or licensed. To the extent the entity licensed the product from a third party, the source code is never available for testing and TT sees no reason why the code should ever be required for testing. The reason why customers purchase turnkey software is to utilize the product as a whole; testing of components of the source code is not consistent with that motivation and doesn't make achieving the goals of the CFTC any more likely.

If TT products do not work as expected, TT's customers demand changes to the products and if TT fails to address their concerns, TT risks losing the customer. In that way companies like TT are effectively "regulated" by the market for software and systems.

We cannot envision any type of testing that would be appropriate with respect to the code itself. If a line by line test of the code to determine whether there are flaws in the way it was written is intended by Regulation AT, it is unclear how any such review would provide any more or better insight than a test of the product itself to see what the outputs are.

Moreover, taking the extraordinary step of mandating testing or review of source code is potentially very damaging to the source code owner as indicated previously.

To the extent third party code is at issue, third party code simply will not be made available to licensees. Neither TT nor any other commercial software vendor that facilitates algorithmic trading licenses source code to its customers and will not willingly do so. We believe, respectfully, that any attempt to mandate third party vendors to produce such code outside of existing legal procedures, such as issuing subpoenas, would be an unprecedented overreach of governmental power without any merit.

Thank you very much for the opportunity to testify before you today. I am happy to address any questions you may have.