

**EXAMINING THE CFTC'S PROPOSED RULE:
REGULATION AUTOMATED TRADING**

HEARING

BEFORE THE

**COMMITTEE ON AGRICULTURE
HOUSE OF REPRESENTATIVES**

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

JULY 13, 2016

Serial No. 114-56



Printed for the use of the Committee on Agriculture
agriculture.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

20-912 PDF

WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

COMMITTEE ON AGRICULTURE

K. MICHAEL CONAWAY, Texas, *Chairman*

RANDY NEUGEBAUER, Texas,
Vice Chairman

BOB GOODLATTE, Virginia
FRANK D. LUCAS, Oklahoma
STEVE KING, Iowa
MIKE ROGERS, Alabama
GLENN THOMPSON, Pennsylvania
BOB GIBBS, Ohio
AUSTIN SCOTT, Georgia
ERIC A. "RICK" CRAWFORD, Arkansas
SCOTT DESJARLAIS, Tennessee
CHRISTOPHER P. GIBSON, New York
VICKY HARTZLER, Missouri
DAN BENISHEK, Michigan
JEFF DENHAM, California
DOUG LAMALFA, California
RODNEY DAVIS, Illinois
TED S. YOHO, Florida
JACKIE WALORSKI, Indiana
RICK W. ALLEN, Georgia
MIKE BOST, Illinois
DAVID ROUZER, North Carolina
RALPH LEE ABRAHAM, Louisiana
JOHN R. MOOLENAAR, Michigan
DAN NEWHOUSE, Washington
TRENT KELLY, Mississippi

COLLIN C. PETERSON, Minnesota, *Ranking
Minority Member*

DAVID SCOTT, Georgia
JIM COSTA, California
TIMOTHY J. WALZ, Minnesota
MARCIA L. FUDGE, Ohio
JAMES P. MCGOVERN, Massachusetts
SUZAN K. DELBENE, Washington
FILEMON VELA, Texas
MICHELLE LUJAN GRISHAM, New Mexico
ANN M. KUSTER, New Hampshire
RICHARD M. NOLAN, Minnesota
CHERI BUSTOS, Illinois
SEAN PATRICK MALONEY, New York
ANN KIRKPATRICK, Arizona
PETE AGUILAR, California
STACEY E. PLASKETT, Virgin Islands
ALMA S. ADAMS, North Carolina
GWEN GRAHAM, Florida
BRAD ASHFORD, Nebraska

SCOTT C. GRAVES, *Staff Director*
ROBERT L. LAREW, *Minority Staff Director*

CONTENTS

	Page
Conaway, Hon. K. Michael, a Representative in Congress from Texas, opening statement	1
Prepared statement	3
Peterson, Hon. Collin C., a Representative in Congress from Minnesota, opening statement	4
WITNESSES	
Wood, Gregory John, Chairman, Market Access Committee, Futures Industry Association; Director, Electronic and Algorithmic Execution, Listed Derivatives, Deutsche Bank Securities Inc., Washington, D.C.	4
Prepared statement	6
Gorelick, J.D., Richard, Chief Executive Officer, RGM Advisors, LLC, Austin, TX	11
Prepared statement	13
Vrabel, J.D., Andrew, Executive Director, Global Head of Investigations, Market Regulation Department, CME Group, Inc., Chicago, IL	20
Prepared statement	22
Ryan, Michael G., Executive Vice President and General Counsel, Trading Technologies International, Inc., Chicago, IL	25
Prepared statement	26
SUBMITTED MATERIAL	
Bergles, Susan, Assistant General Counsel, American Gas Association, submitted statement	65

EXAMINING THE CFTC'S PROPOSED RULE: REGULATION AUTOMATED TRADING

WEDNESDAY, JULY 13, 2016

HOUSE OF REPRESENTATIVES,
COMMITTEE ON AGRICULTURE,
Washington, D.C.

The Committee met, pursuant to call, at 10:00 a.m., in Room 1300 of the Longworth House Office Building, Hon. K. Michael Conaway [Chairman of the Committee] presiding.

Members present: Representatives Conaway, Neugebauer, Goodlatte, Lucas, King, Thompson, Gibbs, Austin Scott of Georgia, Crawford, DesJarlais, Benishek, Denham, LaMalfa, Davis, Allen, Moolenaar, Newhouse, Kelly, Peterson, David Scott of Georgia, Walz, Fudge, McGovern, DelBene, Vela, Lujan Grisham, Kuster, Nolan, Bustos, Kirkpatrick, Aguilar, Plaskett, Adams, and Graham.

Staff present: Caleb Crosswhite, Darryl Blakey, Haley Graves, Kevin Webb, Paul Balzano, Scott C. Graves, Stephanie Addison, Liz Friedlander, Matthew MacKenzie, Nicole Scott, and Carly Reedholm.

OPENING STATEMENT OF HON. K. MICHAEL CONAWAY, A REPRESENTATIVE IN CONGRESS FROM TEXAS

The CHAIRMAN. Good morning. This hearing of the Committee on Agriculture entitled, *Examining the CFTC's Proposed Rule: Regulation Automated Trading*, will come to order.

I have asked Rick Crawford to open us with a quick prayer. Rick. Mr. CRAWFORD. Thank you, Mr. Chairman.

Heavenly Father, we bow humbly before you today, thankful for every blessing of life. Father, thank that we live in this nation that you have provided for us. Father, just ask that everything we say and do here today be pleasing in your sight. Ask it in Jesus' name. Amen.

The CHAIRMAN. Thank you.

Good morning, and welcome again to the hearing on Regulation Automated Trading. Before we get started, I want to thank both Chairman and Ranking Member Scotts. I am not sure how to properly phrase that, David, but you and Austin, and all the Members of the CEEC Subcommittee for their work over the past few months examining Title VII, and working through the ongoing challenges in our derivatives markets. Implementing Title VII has been a monumental task for regulators. The staff and Commissioners of the CFTC deserve credit for their work. Much has been improved over the past 2 years, but clearly, there remains a significant amount of work to be done, especially in harmonizing rules

across borders and fixing outstanding issues like the swap dealer *de minimis* problem.

Over the past 3 decades, our financial markets have been quietly revolutionized by computers. Sometimes called the “electronification” of markets, computer networks have slowly replaced the traditional trading pits. Electronic markets allow computers to seamlessly input orders, giving rise to trading directed and conducted entirely by computer algorithms.

Electronic markets and algorithms offer easier access, reduced transaction costs, and support sophisticated tools that even the smallest market participants can use. Today, algorithmic trading is essential to our futures markets. However, the transition to computers has not been without its challenges. Computer algorithms sometimes interact in unintended ways and markets have suffered disruptions that remain difficult to explain.

In response to this challenging market structure, CFTC staff began work several years ago to address the rise of automated trading across its markets. Since 2012, CFTC staff has held roundtables, participated in advisory committee hearings, put forward a concept release, and no doubt held countless other smaller meetings. Regulation Automated Trading represents the culmination of all this work hard work.

Reg AT is summarized as a comprehensive approach to reducing risk and increasing transparency in automated trading. While I am certainly supportive of reducing risks and increasing transparency, the approach proposed by the Commission falls short of those goals.

Reg AT’s vague boundaries and prescriptive requirements conspire to create a rulemaking that is overly complicated, yet still incomplete. However, the rule does not have to be this complicated. The most confusing parts of Reg AT; the source code rules, the registration regime, the reporting requirements, and the inflexible risk controls, are unnecessary to achieve the Commission’s stated goals. Market participants already have incentives to police bad algorithms, prevent disruptions, and plan for recovery. In many cases, there are already ongoing processes across the industry to impose and refine risk controls.

A more modest proposal by the Commission might start by leveraging these inherent incentives and requiring universal adoption of a flexible framework for best practices.

While I believe the instincts and intentions of the rule are good, its broad scope and sweeping requirements lead me to conclude that it cannot be implemented in its current form. I am heartened that Chairman Massad is open to finalizing the rule in phases, taking more time to get it right. I look forward to seeing the Commission’s next proposal.

I have additional thoughts in my written statement, but for now, let me close by thanking today’s witnesses, each of whom have traveled from out-of-town to be here today. We appreciate your taking the time to prepare the testimony, and your willingness to share your expertise with us, and I want to thank you.

[The prepared statement of Mr. Conaway follows:]

PREPARED STATEMENT OF HON. K. MICHAEL CONAWAY, A REPRESENTATIVE IN
CONGRESS FROM TEXAS

Good morning, and welcome to the Committee's hearing on Regulation Automated Trading.

Over the past 3 decades, our financial markets have been quietly revolutionized by computers. Sometimes called the "electronification" of markets, computer networks have slowly replaced the traditional trading pits. Electronic markets allow computers to seamlessly input orders, giving rise to trading directed and conducted entirely by computer algorithms.

Electronic markets and algorithms offer easier access, reduced transaction costs, and support sophisticated tools that even the smallest market participants use. Today, algorithmic trading is essential to our futures markets. However, the transition to computers has not been without its challenges. Computer algorithms sometimes interact in unintended ways and markets have suffered disruptions that remain difficult to explain.

In response to this changing market structure, CFTC staff began work several years ago to address the rise of automated trading across its markets. Since 2012, CFTC staff has held roundtables, participated in advisory committee hearings, put forward a concept release, and no doubt held countless other smaller meetings. Regulation Automated Trading represents the culmination of all this work hard work.

Reg AT is summarized as "a comprehensive approach to reducing risk and increasing transparency in automated trading." While I am certainly supportive of reducing risks and increasing transparency, the approach proposed by the Commission falls short of those goals.

Requiring firms to provide the CFTC and the Department of Justice with on-demand access to sensitive intellectual property is fraught with danger. There is a legitimate fear among market participants that allowing more people, even regulators, to view and store their intellectual property increases their cybersecurity risks.

While the rule is unclear about the CFTC's intentions, at least one interest group interpreted the rules to suggest that the CFTC will use its newly self-granted authority to "involve itself in the workings of [automated trading systems] to anticipate problems . . ." Such an interpretation of the rule would require CFTC staff to oversee hundreds of algorithmic trading companies, each running dozens of interdependent algorithms, each written with tens of thousands of lines of code. It isn't a stretch to say that using source code to "anticipate problems" in the marketplace would require CFTC analysts to interpret hundreds of millions of lines of code.

The CFTC cannot perform even a fraction of that work in any meaningful way. Yet, absent such a proactive effort to monitor algorithms, it is unclear why else the Commission would require source code be produced without a subpoena.

Reg AT creates a definition, the *AT Person*, to identify the entities covered by the rule which must comply with all of the registration, reporting, testing, compliance, control, and source code repository requirements. Included in that definition are any entities already registered by the CFTC and "engaged in algorithmic trading," as well as those registered as *floor traders*.

Twenty-five years ago, this Committee sought to prevent individuals with felonies from trading in the pits by requiring the individuals trading for their own account in futures pits to register as *floor traders*, be fingerprinted, and undergo background checks.

Under Reg AT, this concept is being re-purposed to try and expand the categories of registered market participants, despite no Congressional change to the current registration requirements.

Beyond the obvious legal question, there is a practical problem to using the *floor trader* definition in this way: the new definition of *floor trader* could wind up *unintentionally* capturing thousands of end-users as *AT Persons*.

Reg AT's vague boundaries and prescriptive requirements conspire to create a rulemaking that is overly complicated, yet still incomplete.

However, the rule does not have to be this complicated. The most confusing parts of Reg AT—the source code rules, the registration regime, the reporting requirements, and the inflexible risk controls—are unnecessary to achieve the Commission's stated goals. Market participants already have incentives to police bad algorithms, prevent disruptions, and plan for recovery. In many cases, there are already ongoing processes across the industry to impose and refine risk controls. A more modest proposal by the Commission might start by leveraging these inherent incentives and requiring universal adoption of a flexible framework for best practices.

While I believe the instincts and intentions of the rule are good, its broad scope and sweeping requirements lead me to conclude that it cannot be implemented in its current form. I am heartened that Chairman Massad is open to finalizing the

rule in phases and taking more time to get it right. I look forward to seeing the Commission's next proposal.

I'll close by thanking today's witnesses, each of whom traveled from out of town to be here today. We appreciate you for taking the time to prepare testimony and your willingness to share your expertise with us. Thank you.

With that, I'll turn to the Ranking Member for his remarks.

The CHAIRMAN. With that, I will turn to the Ranking Member for his remarks. Collin.

**OPENING STATEMENT OF HON. COLLIN C. PETERSON, A
REPRESENTATIVE IN CONGRESS FROM MINNESOTA**

Mr. PETERSON. Thank you, Mr. Chairman, and I thank the witnesses for being here.

A little more than 6 years ago, broad-based stock indexes collapsed and then rebounded over a course of about ½ an hour. The Dow dropped by 998 points in a few minutes, and this was the largest infra-day point decline in its history.

Subsequent research by the CFTC and the SEC determined three factors combined to cause this flash crash: algorithmic trading activity, obscure order submission methods, and an automated trade execution program to sell 75,000 stock index futures.

Since the flash crash, there have been between 15 and 30 similar disruptions every single year in markets ranging from treasuries to crude oil to agriculture futures. With Regulation Automated Trading, the CFTC has proposed some rules to try to prevent future market disruptions caused or made worse by algorithmic trading. This rulemaking is still open, and the CFTC is continuing to work on this, hopefully to get it right.

So I hope that this hearing adds to our understanding of this complex issue, and assists the CFTC in its rulemaking.

I look forward to today's testimony, and I yield back.

The CHAIRMAN. Well, I thank the Ranking Member for his comments.

The chair would request that other Members submit their opening statements for the record so our witnesses may begin their testimony, and to ensure that there is ample time for questions.

We have asked witnesses today who actually have to live with and/or are living with this rule, to give us as close to an insider look at the impact the rules will have as we can.

We have Mr. Greg Wood, Chair, FIA Market Access Committee, Washington, D.C. We have Richard Gorelick, CEO of RGM Advisors, LLC, in Austin, Texas. Andrew Vrabel, Executive Director, Global Investigations, the CME Group, Chicago, Illinois. And Mr. Michael Ryan, the Executive Vice President and General Counsel, Trading Technologies International, in Chicago as well.

Mr. Wood, the floor is yours for 5 minutes.

**STATEMENT OF GREGORY JOHN WOOD, CHAIRMAN, MARKET
ACCESS COMMITTEE, FUTURES INDUSTRY ASSOCIATION;
DIRECTOR, ELECTRONIC AND ALGORITHMIC EXECUTION,
LISTED DERIVATIVES, DEUTSCHE BANK SECURITIES INC.,
WASHINGTON, D.C.**

Mr. WOOD. Chairman Conaway, Ranking Member Peterson, and Members of the Committee, thank you for holding this very timely

hearing on the Commodity Futures Trading Commission's proposed Regulation Automated Trading.

My name is Greg Wood, and I am here today representing the Futures Industry Association. I currently serve as the chair of the FIA Market Access Committee, the co-chair of the FIA Market Technology Division's Automated Trading Committee, and I previously served as President of the FIA Market Technology Division itself.

FIA has been working with the industry since well before the 2010 flash crash to establish safeguards for electronic trading. We have published five documents that include best practices, recommendations for risk controls, as well as the development, testing, and monitoring of trading software.

FIA employed ten working groups devoted to analyzing the feasibility of the CFTC's proposed Reg AT, and provided recommendations for improving the regulation prior to finalization. Our efforts have involved the market participants, the exchanges, the futures commission merchants who act as facilitators for clients seeking to access the cleared derivatives markets, as well as other industry associations that represent various market constituents.

Our efforts have been comprehensive, and are outlined fully within my written testimony, which also includes points that will be discussed further by my fellow witnesses, such as concerns regarding the source code provisions of the proposed rule, as well as the complications that arise from the use of third-party-provided software.

For the sake of time today, I will focus my comments on FCMs and their views, particularly with regards to pre-trade risk controls.

U.S. futures markets have evolved into highly sophisticated electronic markets, and 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. For that reason, 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, not just those of AT persons.

Rather than defining what constitutes an *AT person*, and using an artificially constructed 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. 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. Regulations 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. 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, and 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.

While we believe the CFTC can accomplish its objectives in Reg AT without new registration requirements by applying risk controls to all electronic trading, as previously discussed, we understand that the CFTC is concerned that it may be unable to enforce rules regarding automated trading against non-registrants. Thus, in an effort to be responsive to the CFTC's concerns, FIA has joined with other trade associations to propose a requirement that all electronic trading must pass through the pre-trade controls of a CFTC registrant. These controls are typically in addition to the risk controls provided at the DCM level. The responsibility for implementing the appropriate pre-trade risk controls lies either with the FCM registrant that is facilitating electronic access to the DCM, or 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 clearing member that grants access to the DCM.

Required controls must meet the core principles of being designed to reasonably mitigate the potential for sending orders for too large a size to the DCM, sending orders for a clearly erroneous price to the DCM, and sending too many messages to the DCM.

We believe that the recommended approach I have outlined reflects a thoughtful effort designed to most effectively mitigate disruptions in the ever-evolving markets regulated by the CFTC.

Again, I would like to thank you for holding this important hearing. Oversight of the CFTC is such an important function of this Committee, and we commend you for the time devoted to these matters. I will be happy to answer any questions, following my fellow panelists' testimony.

[The prepared statement of Mr. Wood follows:]

PREPARED STATEMENT OF GREGORY JOHN WOOD, CHAIRMAN, MARKET ACCESS COMMITTEE, FUTURES INDUSTRY ASSOCIATION; DIRECTOR, ELECTRONIC AND ALGORITHMIC EXECUTION, LISTED DERIVATIVES, DEUTSCHE BANK SECURITIES INC., WASHINGTON, D.C.

Chairman Conaway and Ranking Member Peterson thank you for holding this very timely hearing on the Commodity Futures Trading Commission's (CFTC) Proposed Regulation Automated Trading (Reg AT). My name is Greg Wood and I am here today representing the Futures Industry Association (FIA). FIA's members have been extremely engaged in providing input to the CFTC as it seeks to finalize Reg AT. I currently serve as the Co-Chair of the FIA Market Technology Division Automated Trading Committee, the Chair of the FIA Market Access Committee, and I previously served as President of the FIA Market Technology Division.

FIA has been working with the industry since well before the 2010 Flash Crash to establish safeguards for electronic trading. We have published five documents that include best practice recommendations for risk controls, developing, testing and monitoring software, and other protections.

FIA employed ten working groups devoted to analyzing the feasibility of the CFTC's proposed Reg AT and providing recommendations for improving the regulation prior to finalization. Our efforts have involved the trading community, the exchanges, market participants and the futures commission merchants (FCM), who act as facilitators for clients seeking to access the cleared derivatives markets. In March of 2016, FIA filed a comprehensive comment letter to address the various components of the proposal. Subsequently, and in response to a recent CFTC Staff Roundtable, FIA has also worked with the Managed Funds Association, SIFMA Asset

Management Group, and the International Swaps & Derivatives Association (together “the Group”) to present a view that has broad agreement across the industry. Further details can be seen within the Group’s comment letter submitted on June 24th.

Today, I will focus my comments on FCMs and their views, particularly with regards to pre-trade risk controls.

During the course of a recent CFTC Staff Roundtable, Staff sought to elicit suggestions on how to better define Direct Electronic Access (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 designated contract markets (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.

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, not just those of AT Persons.
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.**

I would like to highlight the following **Three** key points that FIA feels should be considered in formulating a regulation that is both scalable and effective:

First, **Risk Controls**. U.S. Futures markets have evolved into highly sophisticated, electronic markets, and 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.¹

Rather than defining what constitutes an AT Person, and using an artificially constructed 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. To be clear, we are not opposed to a regulation category subject to appropriate requirements for that group of registrants; however, we believe defining a particular group of people and applying risk controls only to registrants does not safeguard markets to the full extent the industry believes is needed. To that effect, 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-administered² 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.

¹ 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—including those implemented within third-party vendor systems or exchange provided graphical user interfaces that the FCM has administrative control over.

² 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 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.

It is important to note that the Group believes that market participants not using software that includes FCM-administered risk controls should be 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.³ 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 proposal 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.
- **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 the 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 attempt to completely *prevent* them.**

Based on these points, 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 of Proposal:** 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.
- **Due Diligence Requirement:** An FCM must perform due diligence on any customer to which it grants electronic access to the DCM without going through risk controls administered by the FCM. 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.

³Note that administration of such controls may be delegated by the FCM to another party, such as an introducing broker.

Second, **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. Accordingly, the Group believes that the objectives of the proposed rule 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.

Third, **Source Code**. The Source Code requirement for unfettered access to any firm's intellectual property as proposed is **unprecedented** among regulators and threatens commercially valuable intellectual property and proprietary trading strategies. The Source Code requirement in the proposed rule puts highly proprietary information at risk **without measurable benefits**. 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.

Again, I would like to thank you for holding this important hearing. Oversight of the CFTC is such an important function of this Committee and we commend you for the time devoted to these matters. I will be happy to answer any questions following my fellow panelists' testimony.

APPENDIX

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 ❷ ❸ on attached diagram).

- (b) **An API provided by a third-party software provider for market participants to connect via their infrastructure**, with orders subse-

quently 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.⁴

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 through 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 ❷ ❹ 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 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:

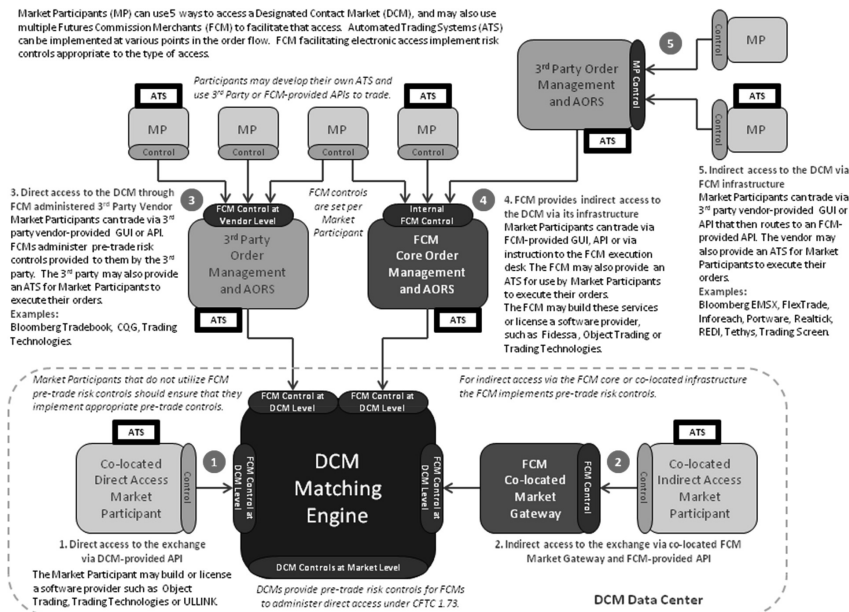
- (a) **An AORS provided by an FCM where orders may be entered via an API or GUI and subsequently routed to the DCM's API** (see ❷ ❹ on attached diagram) using the FCM's membership on the DCM. Such a system may be developed in-house at the FCM or licensed from a third-party provider, but in either situation, 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

⁴Note 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.

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 ① 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.

Sample Pre-Trade Risk Control Locations



The CHAIRMAN. Thank you.
Richard, 5 minutes.

STATEMENT OF RICHARD GORELICK, J.D., CHIEF EXECUTIVE OFFICER, RGM ADVISORS, LLC, AUSTIN, TX

Mr. GORELICK. Thank you, Chairman Conaway, Ranking Member Peterson, and Members of the Committee. Thank you for the opportunity to discuss the CFTC's proposed Reg AT. I will briefly summarize my written statement now, which I ask be included in the record.

I am the CEO of RGM Advisors, a proprietary trading firm that I co-founded in 2001, that trades electronically in a variety of markets. We are based in Austin, Texas, where we employ about 100 people. I serve on the CFTC's Technology Advisory Committee, and

I am involved in industry efforts to enhance trading risk management and public policy. I have advocated for a regulatory environment that promotes fair competition, encourages innovation, improves transparency, manages systemic risk, lowers cost for investors and end-users, and gives regulators the tools that they need to detect and deter abuses.

Mr. Chairman, I support the Commission's stated aims in Reg AT, however, I am concerned that the proposal falls short of achieving them. The rule could amount to a lot of work by the industry and by the Commission, and at best, accomplish only small gains in market integrity. We are fortunate that the industry has already put in place multiple layers of risk controls. New rules should be principles-based and they should be flexible, because technology changes quickly. And since pre-trade risk controls are the most effective safeguard for market integrity, all electronic orders should be subject to them, regardless of the type of market participant or their registration status.

Reg AT tries to accomplish too much in a single regulation. I support the recommendation of commenters to simplify the rule-making by dividing it into separate parts, focusing first on pre-trade risk management.

One part that should be considered separately is the Commission's proposal to create a new requirement for certain market participants to register with the Commission. Setting aside the curious decision to register these automated traders, many of whom never set foot on a trading floor, as floor traders, this requirement is unnecessary to accomplish the Commission's risk management objectives. My written testimony discusses the principles that should guide any automated trading regulation, and includes discussion of several other provisions in Reg AT.

I would like to turn to my concern with the rule's treatment of source code. Source code is an automated trading firm's secret sauce. It comprises very specific and detailed computer instructions that embody the firm's unique trading strategies. Source code often includes valuable trade secrets, developed at significant expense, that directly impact business competitiveness. The requirement to turn over valuable intellectual property to the government on demand would be unprecedented and unreasonable. The proper treatment of IP is central to our private enterprise system. The secret formula for Coca-Cola is not available to the FDA simply upon request. The source code for Google's search algorithms is not available to the government without due process. Government agencies must make a reasonable showing of cause and use a subpoena to get access to private proprietary information. A trading firm's source code should be no different.

For most purposes, source code reviews would be incredibly costly for the CFTC. Trading firms have large and complicated code bases that change regularly. As an example, my relatively small firm has over one million lines of source code associated with our current trading system. We make changes almost daily. To review source code of multiple firms at any scale would require an army of computer programmer regulators. The benefits to the CFTC of reviewing source code would, in most cases, be very limited. It is implausible that reviewing source code as part of an audit or sur-

veillance program would help the CFTC prevent market disruptions, or provide meaningful insight into how a trading system would operate when interacting in a real market. In most cases, surveillance of electronic audit trails presents a much more valuable and cost-effective way to understand trading activity.

I can imagine circumstances in which a regulator would have a legitimate interest in reviewing parts of a firm's source code. However, under those limited circumstances, the regulator should be required to use a subpoena and put in place appropriate safeguards. As we all know, any agency taking possession of source code could raise significant cybersecurity concerns.

Finally, allowing easy government access to source code would set a dangerous precedent with foreign governments, such as China, who seek to impose similar requirements on U.S. firms. We are hopeful that this provision will be revised.

Thank you for the opportunity to testify, and I welcome the Committee's interest in this rulemaking.

[The prepared statement of Mr. Gorelick follows:]

PREPARED STATEMENT OF RICHARD GORELICK, J.D., CHIEF EXECUTIVE OFFICER,
RGM ADVISORS, LLC, AUSTIN, TX

I. Introduction

Chairman Conaway, Ranking Member Peterson, and Members of the Committee, thank you for the opportunity to join you today to discuss the Commodity Futures Trading Commission's (CFTC's or the Commission's) proposed regulation on automated trading, or "Reg AT" as it is commonly known.¹ I am pleased to be with you today to discuss this significant regulatory proposal.

I am the CEO of RGM Advisors, a trading firm located in Austin, TX, that I co-founded in 2001. RGM Advisors is a technology-focused, quantitative trading firm that trades in a variety of equities and futures markets. We use computers to analyze tremendous amounts of market data, to determine what trades we want to make, to conduct those trades, and to manage risk. We have about 100 employees and most of our staff are software developers, information technologists, and quantitative researchers. Most of our software systems have been developed in-house. Our firm, like many in our sector, trades on a proprietary basis, using our own capital to take short-term positions in thousands of instruments.

I serve on the CFTC's Technical Advisory Committee (TAC) and I am a member of the FIA Principal Traders Group (FIA PTG) executive committee. My written testimony today expands on public comments I have shared with the CFTC TAC² and it reflects many of the views that FIA PTG has expressed to the Commission.³

I have been involved in industry-led efforts to develop best practices and guidelines on identifying and mitigating the risks of automated and electronic trading. Since 2010, FIA has published six papers related to these important topics. As a member of the TAC, I have reviewed and commented on CFTC's proposed regulation of automated trading since before the Commission first began considering its initial concept release.

The progression of automated trading has provided substantial benefits to our markets. Increasing automation and competition have helped to improve market quality, increase transparency, and lower costs for investors, hedgers and end-users of all sizes. As we recognize and work to enhance the many benefits of automated trading, we must also ensure that rules and regulations keep pace with technological innovation. I have long been a strong advocate for a regulatory environment that promotes fair competition, encourages innovation, enhances transparency, manages systemic risk, lowers costs for investors and hedgers, and gives regulators the tools they need to detect and deter abuses.

¹ *Proposed Regulation Automated Trading*, 80 FR 78824 (Dec. 17, 2015).

² See http://www.cftc.gov/idc/groups/public/@newsroom/documents/file/tac_022316_transcript.pdf, page 29

³ See https://fia.org/sites/default/files/content_attachments/2016-03-16_Regulation_AT_Comment_Letter.pdf and https://fia.org/sites/default/files/2016-06-24_RegAT_Roundtable_Group_Comment.pdf.

I am supportive of the Commission's stated aims in developing Reg AT, which are to mitigate the risks arising from algorithmic trading activity, to increase transparency with respect to exchange programs and activities, and to update Commission rules in response to the evolution from pit trading to electronic trading. I appreciate the substantial effort put forth by the Commission staff in drafting this proposal.

While these goals are laudable, the proposed rule, as it currently stands, falls short of achieving these goals, and is overly complicated, costly, and confusing. Some aspects of the proposed rule are too broad, while others are too narrow to adequately address risks. I am concerned that the rule could amount to quite a lot of work by the industry and by the Commission to accomplish disproportionately small gains in market integrity, while introducing significant potential negative unintended consequences.

In my testimony, I will first set out generally accepted principles for the regulation of automated trading and then share substantive concerns with proposed Reg AT.

II. Principles for Regulation of Automated Trading

There is broad industry consensus on the principles that should guide any regulation of automated trading.

First, it is critical to recognize and leverage the substantial risk controls and safeguards that have already been put in place by the industry. The CFTC's TAC has provided a forum to explore current industry practices with respect to electronic trading. In addition to detailed discussions of industry best practices for risk management, exchanges (CME and ICE, in particular) have presented thoughtful risk controls and extensive surveillance capabilities in great detail. New regulation should build on the existing framework that has proven successful, and should not try to reinvent that framework.

Second, to be effective and relevant to dynamic market conditions and practices, regulations cannot and should not be overly prescriptive. Instead, as has been the CFTC's historical practice, regulators should adopt principles-based rules that allow for flexibility to distinguish between different activities, business structures, and technologies of market participants, as well as changing market conditions, among other factors. Technology changes quickly, so it is important that the rules are able to stand the test of time.

Third, and most critical, pre-trade risk controls are the most effective safeguard for market integrity. Therefore, they should be applied comprehensively to all electronic orders, not just certain orders submitted by certain types of businesses or submitted through certain types of market access. Simply put, *all* electronic orders should be subject to risk controls, not just those from certain types of market participants. To do otherwise would create loopholes and blind spots.

To be clear, the application of risk controls to every order does not require every market participant to implement its own risk controls. The policy should be to ensure that all orders are subject to appropriate risk controls that can be provided in various ways by market participants, clearing firms, or exchanges.

III. Specific Concerns with Proposed Reg AT

With respect for the CFTC's significant work on this rule, I believe Reg AT tries to accomplish far too much in a single regulation, making it unwieldy and impractical. To address this, I support the idea of simplifying the rulemaking by breaking it up into separate components, in order of importance: (1) pre-trade and other risk controls, (2) policies and procedures for the development, testing, deployment and monitoring of algorithmic trading (including third-party software), and (3) if necessary, registration of certain market participants.

Considering these components separately would allow the Commission to focus first on the parts of Reg AT that are most important to market integrity and widely supported by industry participants: pre-trade and other risk controls. Separating the rulemaking would also allow the CFTC to determine the proper scope for each area of regulation.

My specific concerns with Reg AT fall into the following categories: the scope of the proposal, unnecessary registration requirements, and access to intellectual property, including source code, without due process.

A. The Scope of Reg AT Is Too Broad in Some Parts and Too Narrow in Others

One of the stated goals of the proposed rule is to reduce the risks of automated trading. To accomplish this, it introduces a myriad of requirements, both technical and operational in nature, for newly defined "AT Persons."

Rather than starting from the principle that all electronic orders must be governed by certain risk controls, the rule proposal attempts to cover a limited class

of market participants within the definition of an AT Person. Consequently, the rule would establish a class of market participant that would not be required to have risk controls in place despite having a similar ability to impact market integrity. As a result, the rule may fail in its primary goal of protecting the market.

In other areas, the Commission's proposal is too broad. In particular, the rule would impose a wide range of very specific requirements pertaining to how AT Persons manage their automated trading operations. These requirements include detailed rules for development, testing, documentation, monitoring, training, compliance and reporting across several dimensions of a firm's operations. While some of these requirements roughly track industry best practices, others do not, and most of these requirements are burdensome and do not clearly contribute to market integrity.

As just one example, the proposal includes a provision that would require AT Persons to produce an annual report detailing all changes to their risk settings during the course of a year and to deliver that annual report to the exchanges on which they traded. It is not unusual for firms trading hundreds of products to change their risk limits multiple times per day. These changes are often made in an exchange-based interface managed by a clearing firm, and as a result, the clearing firm and the exchange know about the risk limit changes in real time. While it would amount to a lot of work for AT Persons to produce these annual reports and for exchanges to review them, it is hard to see what additional information would be communicated in the process, or how risk management would be improved. Such onerous requirements would both inhibit an AT Person's ability to innovate compared to non-AT Persons with similar businesses, and also dramatically increase the cost of maintaining algorithmic trading operations. These costs would certainly be passed on to market end-users in the form of higher transaction costs and less liquid markets.

Moreover, some of the proposed definitions are, in my opinion, too broad and, as a result, may be counterproductive. Much of the proposed rule is geared toward preventing "Algorithmic Trading Events" which are defined to include both "Algorithmic Trading Compliance Issues" and "Algorithmic Trading Disruptions." As a result of these definitions, the more comprehensive a firm's policies, the more liability it would risk if any practice were found to have varied from its written policy. Rational actors would be incented to have fewer internal controls, rather than more. Similarly, the rule would prohibit firms from "disrupting or materially degrading" their own trading. This requirement might encourage firms to continue trading in the face of potential risk management issues. In my opinion, those provisions should be eliminated from their respective definitions.

B. The Registration Requirements Are Unnecessary

The CFTC is proposing to create a new requirement for certain market participants trading solely for their own account and using automation to register with the Commission as floor traders. Setting aside the curious decision to register these automated traders, many of whom never set foot on a trading floor, as "floor traders," this requirement is unnecessary. Exchange rules and industry best practices already require some types of pre-trade risk management for all market participants regardless of registration category. The trading activity by the market participants that would be covered by this requirement is already managed through exchanges and there is no gap in risk controls. The CFTC has the legal authority and should apply appropriate risk management requirements broadly to all market participants whether or not they are registered with the Commission.⁴

I support comments by FIA, FIA PTG, and other industry associations explaining that registration requirements are unnecessary. I reiterate that any market participant, regardless of registration status or type of trader, has the potential to disrupt markets. It should be noted that when the SEC studied market disruptions (or so-called mini-flash-crashes) they noted that the majority of such events were caused by human mistakes, such as fat-finger errors, rather than algorithmic trading bugs. In addition, if the Commission would start from the basic principle that all electronic orders should be subject to risk controls, and that these requirements should not hinge on registration status, the entire rule would become much less complex to design and implement.

⁴The Commission already has ample legal authority to impose requirements on non-registrants that trade on U.S. futures markets in order to prevent disruptive practices expressly described in Section 4c(a)(5) of the Commodity Exchange Act ("CEA"), as well as "any other trading practice that is disruptive of fair and equitable trading." Using this authority, the CFTC has a statutory basis to enact rules to require all traders (whether registered as AT Persons or not) to comply with requirements meant to avoid prohibited conduct.

Should the CFTC be determined to implement a new registration requirement, then such registration should be considered separately and apart from the proposed pre-trade risk controls in proposed Reg AT, so its potential effects can be given full and careful consideration. Any registration requirement should be based upon a new and more suitable registration category rather than over-loading the existing “floor trader” category created for individual market participants standing on a trading floor.⁵ At a minimum, the Commission should delay adoption of any registration requirement until after it has implemented other components of Reg AT to evaluate the necessity of registration, which would be costly for new registrants and the Commission, and would be a burdensome distraction for the National Futures Association (NFA).

C. Source Code Should Only be Available to the Government with Due Process

The final concern I would like to raise today is the CFTC’s proposed access to source code. The proposed requirement to turn over valuable intellectual property (IP) to the government on demand is simply unprecedented and unreasonable. The proper treatment of IP lies at the heart of our private enterprise system. As noted by CFTC Commissioner Giancarlo in connection with the issuing release for Reg AT,⁶ the secret formula for Coca Cola is not available to the FDA, certainly not on demand. The source code for Google’s search algorithms is not available to the government without due process. Government agencies must make a reasonable showing of cause and get a proper court order, such as a subpoena, to gain access to intellectual property.

A trading firm’s source code should be no different. Most modern trading firms are very much technology businesses. Many of our staff write software, and our source code constitutes important trade secrets and valuable IP about our future business plans. Modern trading firms invest significant time, effort and money in technological innovation, much of which is embodied in source code, and they go to great lengths to protect its confidentiality and their competitive edge. Not only would this proposed provision set a troubling precedent for government access to private information, but it would do so without any demonstrable regulatory benefits to offset the significant risk associated with the misappropriation of that intellectual property.

Proposed Reg AT would accomplish this unprecedented access by classifying source code as “books and records” which would make them available to the Commission and the Department of Justice upon request. Source code, however, is unlike other books and records such as trade blotters and similar records, which can be reasonably protected with standard confidentiality. Source code often is comprised of valuable trade secrets that represent substantial investment and innovation and can directly impact the competitiveness of a business.

It should be recognized that for most purposes, source code reviews would be incredibly costly for the CFTC. Trading firms have very large and complicated code bases that change very often. As an example, my firm is a relatively small trading firm. We have over a million lines of source code associated with our current trading systems. This code has been written over 15 years in about ten different programming languages. We make changes of one kind or another almost daily. To review source code of multiple firms at any scale would require an army of computer programmer regulators.

The benefits to the CFTC of reviewing source code would, in most cases, be very limited. It is not plausible that reviewing source code as part of an audit or surveillance program would somehow help the CFTC prevent future market disruptions or provide any meaningful insight into how a trading system would operate in a real market when interacting with other traders in different market conditions. In most cases, surveillance and analysis of electronic audit trails (such as orders, fills, and cancellations) would present a much more valuable and cost effective way to understand trading activity.

⁵ See <http://comments.cftc.gov/PublicComments/ViewComment.aspx?id=60765> (“Even if the Commission disagrees and decides that registration is necessary to ensure compliance with the Proposal, CME Group questions whether the Commission has sufficient legal authority under the CEA to require registration as a ‘floor trader’ of a new type of distinctly non-floor trader. Historically, the scope of CFTC registrants has only been expanded when Congress provides the Commission with new statutory authority. [. . .] In the absence of such new authority from Congress, the Commission proposes to introduce otherwise unregistered algorithmic traders who access an exchange through DEA into an existing statutory registration category. CME Group is not persuaded by the Commission’s argument that Congress could have intended for the definition of ‘floor trader’ to include only this subset of algorithmic traders.”)

⁶ See <http://www.cftc.gov/ide/groups/public/@newsroom/documents/file/transcript112415.pdf>, page 39.

I can imagine circumstances in which a government agency, such as the CFTC, would have a legitimate interest in reviewing parts of a firm's source code. For example, in an enforcement action for market abuse, reviewing portions of source code might provide some insight into the intent behind the placement of certain orders. However, under those limited circumstances, the Commission should be required to get a subpoena, and put in place appropriate safeguards. To the extent that the CFTC takes possession of any source code, this would raise significant information security concerns.

Moreover, allowing easy government access to source code would set a dangerous global precedent with foreign governments, such as China, who are seeking to impose similar source code requirements on U.S. firms. In fact, the Federal Government recently emphasized 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. This development has not gone unnoticed. In fact, a number of technology and business-focused industry organizations have raised this exact point in formal comments to the CFTC.⁷

We are hopeful that this provision will be revised. CFTC Chairman Massad has indicated that the Commission "take[s] very seriously the fact that [the information] is proprietary, it is significant of value to firms, and . . . [we] would certainly . . . do everything [the CFTC] can to protect confidentiality."⁸ As such, the 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.

I understand that some regulators have worried that trading firms might not adequately retain their source code in such a way that they could make it available for inspection. While good software development practices already lead firms to retain their source code in software control systems, I believe it would be helpful for the Commission to work with industry groups to establish a principles-based retention policy for source code based on current practices that would ensure regulators have access to source code information when needed.⁹ This would allow businesses to maintain control over their sensitive intellectual property while ensuring regulators can access information that they desire, after following appropriate processes.

IV. Conclusion

Altogether, proposed Reg AT would impose costly burdens on market participants, without commensurate benefits. Our markets are dynamic and constantly changing. Mandated risk controls, like those in Reg AT, which are overly specific, could quickly become obsolete as markets, technology, and trading strategies evolve. Creating checklists and written policies might give the appearance of reform, but in practice, do not make markets safer or more resilient—and could instead create unintended incentives to the contrary.

The trading community has a direct interest in well-functioning and resilient markets. We want to comply with the rules of the road. We welcome improvements that actually make the markets safer and more efficient. However, when rules serve to impede those goals, we need to reconsider them. I am concerned that proposed Reg AT, as designed, would not accomplish its stated objective of protecting market integrity, because it would leave many electronic orders outside of its scope. Moreover, this proposed regulation, as currently written, would be costly for market participants and the Commission. These costs would ultimately be borne by market end-users in the form of higher transaction costs and less liquidity. Finally, the source code access provisions put valuable American intellectual property in jeopardy, are without precedent, and would have a chilling effect on technology both inside and outside of the derivatives world.

I appreciate the opportunity to testify before you today and I welcome the Committee's interest in consideration of this rulemaking. I look forward to answering any questions you may have.

Thank you.

[ATTACHMENT]

June 24, 2016

Via CFTC Website: <http://comments.cftc.gov>

⁷ See <http://comments.cftc.gov/PublicComments/ViewComment.aspx?id=60890&>.

⁸ See <http://www.cftc.gov/idx/groups/public/@newsroom/documents/file/transcript061016.pdf>, pages 295–296.

⁹ See https://fia.org/sites/default/files/2016-06-24_RegAT_Roundtable_Group_Comment.pdf, page 9–10.

CHRISTOPHER KIRKPATRICK,
Secretary of the Commission,
 Commodity Futures Trading Commission,
 Washington, D.C.

RE: RIN 3038-AD52—Joint coalition comments in response to CFTC Proposed Regulation AT source code provisions

Dear Mr. Kirkpatrick:

The U.S. Chamber of Commerce (the “Chamber”), the Information Technology Industry Council (“ITI”), the Business Software Alliance, the International Swaps and Derivatives Association, the Futures Industry Association (“FIA”), the FIA Principal Traders Group, Modern Markets Initiative, and the Software & Information Industry Association write to you in strong opposition to the source code disclosure and retention requirements contained in the Commodity Futures Trading Commission’s (the “CFTC”) notice of proposed rulemaking on Regulation Automated Trading (“Regulation AT”)¹ and urge you to entirely eliminate these requirements from the final version of the rule.

In short, if not significantly amended, the proprietary source code provisions of Regulation AT will:

- (1) compromise the established and expected due process rights of our members;
- (2) increase the threat of “copycat” measures from other countries and contradict established U.S. policy on intellectual property disclosure;
- (3) heighten the possibility of cyberattacks against government-mandated data repositories; and
- (4) do little to assist the CFTC in its market surveillance activities.

While this letter is not an exhaustive listing of all of the issues of our associations may have with Regulation AT, we believe that it is important that the CFTC appreciate the broad-based opposition we have to Regulation AT’s proprietary source code provisions.² We elaborate in additional detail below.

Mandating On-Demand Access to Proprietary Source Code Tramples Fundamental Due Process Rights and Attracts Similar Global Responses

Our chief concern with Regulation AT relates to the unprecedented, on-demand access that the CFTC would have to the proprietary source code of market participants engaged in algorithmic trading. Simply put, the proposed requirements force the disclosure of valuable intellectual property to the government based only on a showing that is akin to a document request. That type of requested access contradicts widely held expectations of due process associated with highly sensitive intellectual property—and, indeed, the legal protections that apply to any intellectual property in the U.S.

While the CFTC has recently acknowledged these concerns at a staff roundtable, there is no clear explanation as to why the CFTC could not use well-established U.S. judicial process to obtain access to proprietary source code data when needed. The CFTC and the DOJ have long used subpoenas to obtain access to non-public information and can continue to do so here. However, Regulation AT would provide an end-run around these important protections, eroding the important due process rights of these market participants.

Even more concerning is the precedent that the Regulation AT source code provisions would set, which may invite similar requirements in other countries. As recently as last year, the United States pushed back against a comparable proposal issued by the China Banking Regulatory Commission, which would have required American companies selling computer equipment to Chinese banks to turn over intellectual property and submit source code.³ This action is also consistent with the U.S. Government’s policy against source code disclosure requirements in other contexts, as evidenced by previous opposition to proposed regulations issued by India’s Department of Telecommunications relating to 2009–2010 Telecom Network Equipment Certification requirements, and by Korea’s National Intelligence Service in

¹ Commodity Futures Trading Commission, 80 *Fed. Reg.* 242 (proposed Dec. 17, 2015) (to be codified at 17 CFR Parts 1, 28, 40, *et al.*).

² For additional detail, please see letter of March 16, 2016 to CFTC on Proposed Regulation AT source code provisions, available at the following link (<https://www.itic.org/dotAsset/469665b9-7552-4763-9569-b835eb81a585.pdf>).

³ Paul Mozur and Jane Perlez, *China Halts New Policy on Tech for Banks*, N.Y. TIMES, Apr. 16, 2015, available at http://www.nytimes.com/2015/04/17/business/international/china-suspends-rules-on-tech-companies-serving-banks.html?_r=0.

2005 relating to sales of information security software to Korean Government agencies. Moreover, the signatories to the Trans-Pacific Partnership have also agreed not to require the transfer of, or access to, source code of software owned by a person of another party as a condition for the import, distribution, sale, or use of such software.⁴

These policy decisions from other parts of the U.S. Government demonstrate a strong expression of U.S. Administration policy to defend the rights of intellectual property holders from unnecessary disclosure to third parties, including government entities. It also signals the extent to which the CFTC is a relative outlier compared to other financial services and capital markets regulators, and certainly with respect to other instrumentalities of the U.S. Government. We believe that the CFTC should follow these decisions when finalizing Regulation AT, recognize the important of intellectual property to these firms, and respect the due process rights of its regulated entities.

Mandating On Demand Access to Proprietary Source Code Is Inefficient and Will Not Assist the CFTC

Proprietary source code data is extremely difficult to understand without its developer, and simply viewing the source code on demand would not assist the CFTC in determining if automated trading contributed to a market-wide event. Participants at the CFTC's roundtable on June 10 noted that source code differs substantially from "books and records" requirements, in that proprietary source code does not solely provide information on instructions. Instead, it tells the story behind "why" and "how" a decision is made—much of which is impossible to understand without recreating a scenario event with the assistance of a developer.

Consequently, we fail to see how the CFTC's on demand access requirements will actually assist the agency in its market surveillance and investigative activities. In addition, the CFTC has not provided an estimate of the costs for hiring qualified developers that could actually analyze the proprietary source code, meaning that the CFTC currently does not know how much it would even cost to review information within its possession. We question the value of requesting on demand access to proprietary source code when the CFTC may not even have the resources to analyze it.

Regulation AT Increases the Potential for Cyberattacks and Threatens the Security of Proprietary Source Code

As proposed, Regulation AT requires automated trading firms to maintain source code repositories to manage source code access, maintain copies of production code (as well as logs of changes to production code), and include an audit trail to determine who made changes to source code, under what circumstances, and why.⁵ Such repositories must be available for inspection by the CFTC, the DOJ, and potentially third parties.

We strongly object to mandating automated trading firms to create source code repositories under the terms established by Regulation AT, especially when many companies already maintain such information. Moreover, establishing the same across-the-board requirement unintentionally makes those repositories "cyber targets," giving hackers and others a precise location for obtaining an automated trading firm's most valuable intellectual property.

Moreover, there is substantial reason to believe that proprietary source code data would not be safe in a government-mandated repository or in the hands of the Federal Government. In the past year, we have seen cyberattacks against the Internal Revenue Service,⁶ the Office of Personnel Management,⁷ the Federal Deposit Insurance Company,⁸ and the Board of Governors of the Federal Reserve.⁹ Even the

⁴See Article 14.17: Source Code, Trans-Pacific Partnership (ICT Annex), available at <https://ustr.gov/sites/default/files/TPP-Final-Text-Electronic-Commerce.pdf>.

⁵See *supra* note 1 at p. 78824.

⁶Stephen Dinan, *IRS hit by cyberattack, thousands of taxpayers' information stolen*, THE WASHINGTON TIMES, May 26, 2015, available at <http://www.washingtontimes.com/news/2015/may/26/irs-hit-cyberattack-thousands-taxpayers-information/>.

⁷Julianne Pepitone, *Federal Data Breach: Can the Government Protect Itself From Hackers?*, NBC NEWS, Jun. 5, 2015, available at <http://www.nbcnews.com/tech/security/federal-data-breach-can-government-protect-itself-hackers-n370556>.

⁸Joe Davidson, *FDIC cyberattacks included hit on former chairwoman's computer*, THE WASHINGTON POST, May 11, 2016, available at <https://www.washingtonpost.com/news/powerpost/wp/2016/05/11/fdic-cyberattacks-included-hit-on-former-chairmans-computer/>.

⁹David Murphy, *House Committee Investigates Federal Reserve Cyber-Attacks*, PC MAG, Jun. 4, 2016, available at <http://www.pcmag.com/news/344991/house-committee-investigates-federal-reserve-cyber-attacks>.

CFTC suffered its own data breach in June of 2012, risking the security of its employees' [S]ocial [S]ecurity [N]umbers.¹⁰ Given how incredibly valuable proprietary source code data would potentially be in the hands of a hacker, we believe that these data breaches are enough reason for the CFTC to eliminate this element of Regulation AT.

Conclusion

While we appreciate the CFTC's need for timely access to data in order to fulfill its market surveillance mission, the proprietary source code requirements of Regulation AT are a bridge too far. By mandating on demand access to proprietary source code and the development of source code repositories, the CFTC not only compromises established due process rights—it also adopts policy in direct contradiction to other agencies of the U.S. Government and increases the risk of cyberattack, all while not providing any tangible benefit to the CFTC. Consequently, we believe that the proprietary source code provisions of Regulation AT should be eliminated in their entirety.

Sincerely,

BSA/The Software Alliance;
Information Technology Industry Council;
International Swaps and Derivatives Association;
Futures Industry Association;
FIA Principal Traders Group;
Modern Markets Initiative;
Software & Information Industry Association;
U.S. Chamber of Commerce.

The CHAIRMAN. Thanks, Richard.

Mr. Vrabel, 5 minutes.

STATEMENT OF ANDREW VRABEL, J.D., EXECUTIVE DIRECTOR, GLOBAL HEAD OF INVESTIGATIONS, MARKET REGULATION DEPARTMENT, CME GROUP, INC., CHICAGO, IL

Mr. VRABEL. Thank you, Chairman Conaway, Ranking Member Peterson, and Members of the Committee. My name is Andrew Vrabel, I am the Global Head of Investigations at CME Group where my teams are responsible in part for monitoring CME's markets for aberrant market activity, including activity that may be the result of automated trading strategies.

I am pleased to be here today to discuss the CFTC's proposed rule on automated trading, referred to as Reg AT. As many of you may be aware, automated trading strategies, or algorithmic trading, is a source of considerable liquidity in today's markets. These are strategies that are used by all types of participants, from commercial end-users to market makers, for price discovery and efficient risk management. But like any automated process, there are inherent risks associated with automated trading, and it is because of this, and CME Group's vested interest in preserving the integrity of our markets, that we have pioneered innovative market controls, and have devoted substantial resources to protect the market from potential aberrations and disruptions.

On top of these measures, which have proven highly effective over time, Reg AT aims to mandate additional tools and controls which we, unfortunately, think are broad, unworkable, and could be counterproductive.

¹⁰Silla Brush, *CFTC Data Breach Risks Employees' Social Security Numbers*, BLOOMBERG NEWS, June 25, 2015, available at <http://www.bloomberg.com/news/articles/2012-06-25/cftc-data-breach-risks-employees-social-security-numbers>.

One particular area of Reg AT that we have concerns with is a requirement that the exchanges implement tools and controls that would prevent algorithmic traders from committing a disruption in the marketplace. Unfortunately, this is an unachievable standard. The most robust tools imaginable cannot prevent all algorithmic trading disruptions, or all disruptions in the markets, for that matter. Instead, we have proffered to the CFTC, and we believe that the exchanges, if required to do anything, should be to create tools and controls that would mitigate rather than prevent the potential for an algorithmic trading disruption in the markets.

Relatedly, Reg AT would also require the exchanges to implement tools that would prevent traders from committing compliance violations, most of which is already prohibited by the Commodity Exchange Act, carrying criminal penalties, and is also prohibited by CFTC's regs and exchange rules. The exchanges have never been asked to mandate or create a control that would guarantee universal compliance. In my experience, people intent on violating the law will find a way to do so, whether there is a control in place or not. It is for this reason we have asked the CFTC to abandon this portion of Reg AT in its entirety.

Reg AT also proposes that the exchanges review extensive compliance reports to identify and remediate deficiencies with risk controls, development, and testing standards. The weakness with this particular approach is that the information contained in those compliance reports is backward-looking. It will, therefore, be stale the moment the exchanges have an opportunity to review it. Beyond that, even if the exchanges are asked to review these extensive compliance reports, in order to do a substantive review of this type of information, it will require highly specialized skills and knowledge that, in our experience, is only possessed by the traders and firms that created the algorithms themselves. The exchanges are not suited, nor should they be, to perform this type of review on a regular basis. Instead, we believe that the clearing member firms that grant that particular participant access to the market is in a strong position to receive from that trader or trading firm a certification or a verification that they are in compliance with the requirements of Reg AT. Then, if necessary, the exchanges can ascertain the veracity of those certifications and verifications.

One notable void in Reg AT with respect to market risk controls is that Reg AT would mandate them for only a certain subset of algorithmic traders; the so-called AT persons. The reason for this void we believe is that the CFTC is primarily intent on capturing a set number of new registrants. We believe that registration is a secondary concern that, if at all, should be addressed in a separate rulemaking. Instead, we think that the goal of Reg AT should be on the creation of flexible, not-mandated, market-wide risk controls that apply to every algorithmic trader order that is submitted to the exchange.

We, therefore, submitted to the CFTC a proposal or an idea of a two-tiered system of market risk controls. One tier of risk controls could be administered by the algorithmic trader themselves or the clearing firm that provides them access to the marketplace, and another level of risk controls would be administered by the exchange on a market-wide basis. These two levels of control would

provide the marketplace adequate, necessary, and maximum protections from the potential of an algorithmic trading disruption.

Last, you have heard from others and you will hear more on source code. I will keep our comment here specific and limited. The Commission has administrative subpoena authority under the Commodity Exchange Act, and this affords participants due process and a mechanism to preserve the confidentiality of that information. Given the sensitivity of source code, we see no reason why this approach shouldn't be adequate to the CFTC on a going forward basis.

While the concerns we raise with Reg AT are significant, we are hopeful that the CFTC continues to work with the marketplace as they have to create a better and stronger rule.

On behalf of CME Group, I truly appreciate the opportunity to be here, and I look forward to answering any questions that you may have.

[The prepared statement of Mr. Vrabel follows:]

PREPARED STATEMENT OF ANDREW VRABEL, J.D., EXECUTIVE DIRECTOR, GLOBAL HEAD OF INVESTIGATIONS, MARKET REGULATION DEPARTMENT, CME GROUP, INC., CHICAGO, IL

Thank you, Chairman Conaway, Ranking Member Peterson and Members of the Committee.

My name is Andrew Vrabel. I am the Executive Director of Global Investigations at CME Group, which is part of our Market Regulation division. I am pleased to present CME Group's views on the CFTC's proposed rules to enhance regulation of algorithmic trading, known as "Regulation AT."¹

Algorithmic trading, a type of automated trading, is a source of considerable market liquidity today, facilitating price discovery and efficient risk management. Yet, as with any automated process, there are risks associated with algorithmic trading. To preserve and protect the integrity of our markets from these risks, CME Group has pioneered innovative risk controls and system safeguards, and continually employs substantial human resources and technological capabilities for the development, implementation and enhancement of these controls. In my role, I see first-hand every day the sophisticated tools our exchanges have developed and use to mitigate risks and protect our markets.

Regulation AT aims to mandate additional standards for protections on top of the strong self-regulatory measures that our exchanges already apply. We are concerned that much of Regulation AT's framework is overly broad in scope, unworkable and could be counterproductive. Our comment letters urge the CFTC to re-focus its proposal on the essential area of flexible, not mandated, market risk controls that can be tailored to the different business operations and roles of traders, intermediaries and exchanges to best protect market integrity.² Getting Regulation AT right is critically important to all who use our markets.

We identify the following key areas where the proposed rulemaking needs to be substantially refined:

Regulation AT Should Not Require a Designated Contract Market ("DCM" or "Exchange") To Prevent Algorithmic Trading Disruptions or Algorithmic Trading Compliance Issues

Our primary concern is that Regulation AT appears to require exchanges to prevent Algorithmic Trading Disruptions ("algorithmic trading disruptions").³ As CFTC Chairman Massad, observed when approving the Proposal, no control—like no

¹ See *Regulation Automated Trading*, 80 FED. REG. 78824 (December 17, 2015); see also *Public Staff Roundtable on Elements of Regulation Automated Trading: Reopening of Comment Period*, 81 FED. REG. 36484 (June 7, 2016).

² See Letter from CME Group to CFTC, re: Notice of Proposed Rulemaking on Regulation Automated Trading (RIN 3038-AD52), dated March 16, 2016. See Letter from CME to CFTC re: Reopening of Comment Period re: Regulation Automated Trading (RIN 3038-AD52), dated June 24, 2016.

³ As used herein, "Algorithmic Trading Disruption" has the meaning contained in the Proposal.

rule—can always prevent disruptions and other operational problems that may arise from algorithmic trading.⁴ We agree. As a result, we believe the “prevent” standard is unachievable. Instead, we urge the CFTC to adopt a standard that requires exchanges to implement tools to *mitigate* the effects of an algorithmic trading disruption. Any final rule text and accompanying preamble should consistently articulate this achievable objective for exchanges.

Regulation AT also appears to require exchanges to *prevent* Algorithmic Trading Compliance Issues (“algorithmic trading compliance issues”).⁵ The Proposal would require exchanges to prevent an event that causes a certain trader to operate in a manner that does not comply with the Commodity Exchange Act or its rules and regulations, rules of any exchange to which such algorithmic trader submits orders through algorithmic trading, the National Futures Association rules, the algorithmic traders own internal requirements, or the requirements of the trader’s clearing firm. We oppose this requirement for two reasons. First, as discussed below, we believe Regulation AT generally should not attempt to address compliance issues, but should instead focus on deterring algorithmic trading disruptions. Second, imposing this type of universal compliance obligation on DCMs is a major departure from DCMs’ traditional self-regulatory role Congress envisioned, as reflected in the Core Principles.⁶

Exchanges have never been asked to guarantee, or provide tools to guarantee, the universal compliance by certain market participants because such a requirement would be unrealistic and unreasonable. People who intend on violating the law, Federal regulation, or rule of a self-regulatory organization will find a way. Further, requiring an exchange to guarantee compliance and prevent algorithmic trading compliance issues could inadvertently create a safe-harbor in an enforcement action. If a trader or firm subsequently is accused of violating an exchange rule, CFTC regulation, or provision of the Commodity Exchange Act, they could cite to an exchange’s prior action (or inaction) in defense of the allegations. This could significantly undermine the effectiveness of an enforcement program and disciplinary action.

What has proven effective is when exchanges operate in the self-regulatory role Congress envisioned, which includes adopting and enforcing rules of conduct related to trading. This serves to not only penalize wrongdoers where warranted but also to deter other would-be violators, whether they deploy algorithmic trading strategies or are manual, point-and-click traders.

Requiring Exchanges To Review and Evaluate Annual Compliance Reports, Policies, and Procedures and Enforce Compliance With Regulation AT Is Unworkable and Beyond the Scope of an Exchange’s Role

CME Group believes the Commission’s proposed requirement that certain algorithmic traders prepare and submit extensive annual compliance reports to exchanges creates an unnecessary administrative burden and substantial costs on all parties involved without providing significant benefit to market integrity. There are many reasons that support removing this aspect of the Proposal. First, the information contained in the proposed compliance reports would be stale and not representative of how a firm is currently addressing risks by the time the reviews are submitted to an exchange. This renders the exchange review substantially ineffective at preventing or mitigating a future algorithmic trading event.

Second, exchanges are not practically in a position to assess an algorithmic trader’s compliance with Regulation AT or issue remediation instructions. Assessing pre-trade risk controls designed to prevent or even mitigate an algorithmic trading event will be dependent on granular aspects of each algorithmic strategy, including inputs, variables, and calculations that inform the strategy; system architecture; operational infrastructure; and the skills and experience of each trader, programmer, and developer. Not only is this information highly sensitive and proprietary, but assessing these aspects will require highly specialized skills and knowledge possessed only by the traders or firms themselves.

Finally, under the Proposal, a DCM’s review of a compliance report and remediation instructions, if any, would seemingly endorse the policies, procedures, and risk control parameters. This imposes significant liability on the exchanges, and again, it potentially creates a safe-harbor if an issue subsequently arises.

⁴ See Chairman Massad’s Statement on November 24, 2015 (<http://www.cftc.gov/PressRoom/SpeechesTestimony/massadstatement112415>).

⁵ As used herein, “Algorithmic Trading Compliance Issues” has the meaning contained in the Proposal.

⁶ See Section 5(d) of the Commodity Exchange Act.

As the Commission is well aware, the CME Group exchanges rigorously scrutinize the trading on our markets each day pursuant to our commitment to protecting the integrity of our markets and complying with existing DCM core principle requirements. We routinely monitor the market and conduct exhaustive reviews of market events and other conduct that might be considered disruptive. As a matter of practice, if an algorithm malfunctions and causes a disruption in the market, we conduct an in depth review of the participant's risk controls, development and testing procedures, and compliance policies. We submit that this is the proper role of an exchange and that the Commission should not force exchanges to change these well-functioning mechanisms as a result of Regulation AT.

To the extent verification of an algorithmic trader's compliance is needed, we believe the clearing member that granted the trader access to the exchange would be better positioned to accept a certification of compliance as a condition precedent to granting that trader access to the market.

We believe that a refined focus on the risk of market disruptions, *e.g.*, algorithmic trading disruptions, would enable the Commission to establish a coherent and meaningful framework to address the risks presented by algorithmic trading.

Pre-Trade Market Risk Controls Applied to all Algorithmic Traders

CME Group proposes that two layers of pre-trade risk controls would apply to all algorithmic trading orders. The first layer would be administered by either the algorithmic trader itself or its clearing member that granted access to the exchange. The second layer would be developed and administered by the exchange. Both layers of market risk controls must be reasonably designed to mitigate the effects of algorithmic trading disruptions, and set at a level of granularity appropriately tailored to the underlying nature of the algorithmic trading activity such that the risk mitigation standard is met.

CME Group believes that *all* algorithmic traders should be subject to market risk controls. Proposed Regulation AT leaves a control void for some algorithmic traders by only requiring market risk controls for, the so-called "AT Persons."⁷ The reason for this gap is that the CFTC has focused primarily on attempting to capture a set number of new registrants. We believe registration is a secondary concern—the first aim of any rule in this area should be establishing a blanket of market risk controls that applies to all algorithmic trading in a consistent manner.

We also believe the long-term effectiveness of any market risk control framework is dependent upon market participants being afforded flexibility to innovate as trading technology evolves. Accordingly, CME Group's alternative framework would not mandate the use of any specific market risk control measures. Rather, the rules would establish acceptable practices that market participants can follow in order to meet the applicable risk mitigation standard, consistent with the Commission's history of establishing acceptable practices in other areas of DCM core principle compliance.

The Source Code Open Access Requirement Raises Serious Confidentiality Concerns

Other industry representatives will testify about the source code issue. We agree with those who want to avoid undue, routine disclosure of their intellectual property to government officials. This provision raises serious concerns regarding the confidentiality of proprietary information. Currently, if the Commission has reason to believe that it needs access to a market participant's source code, it can obtain the code subject to adequate confidentiality protections via the subpoena process. We know of no reason why this approach should not be satisfactory to the CFTC given the sensitivity of the information at issue.

* * * * *

CME Group appreciates the opportunity to share our views on this important rule proposal. We remain hopeful that the CFTC will continue to work with all stakeholders to build a stronger and better rule.

I look forward to answering any questions you might have.

The CHAIRMAN. Thank you.

Mr. Ryan, 5 minutes.

⁷ As used herein, the term "AT Person" has the meaning contained in the Proposal.

**STATEMENT OF MICHAEL G. RYAN, EXECUTIVE VICE
PRESIDENT AND GENERAL COUNSEL, TRADING
TECHNOLOGIES INTERNATIONAL, INC., CHICAGO, IL**

Mr. RYAN. 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 of Trading Technologies International. We are commonly known as TT in the industry.

TT is an independent software vendor, or ISV, of approximately 400 employees. Our headquarters are in Chicago, and we have offices in most of the major financial centers around the world.

TT licenses electronic trading systems that enable its customers to trade on the 45 major electronic exchanges and liquidity platforms globally. TT's products, which are housed at our customers' facilities or hosted by TT in co-location facilities, enable customers to trade using several automated tools, pointing and clicking on a market, or by inputting and utilizing their own proprietary algorithms to trade on electronic exchanges.

As an ISV, I believe that TT provides a perspective on some of the issues related to the proposed Reg AT that is different than many of the other market participants represented here today. In that regard, I appreciate the opportunity to testify about some practical aspects of the regulation, and how it might be implemented using technology in place today.

I will testify on the following three aspects of Reg AT: definition of *direct electronic access*, or DEA; the need for and propriety of a source code repository; and the testing requirements related to electronic trading applications. These are also addressed in my written testimony, which I ask to be included in the record.

TT believes that the definition of *DEA* in Reg AT should be clarified to indicate that there is no direct electronic access where the orders are routed to an exchange through a clearinghouse member's trading system, where pre-trade and other risk controls can be controlled by such a member, even where a trading firm or a third party maintains the physical location of the systems. Without clarifying the language, the definition of *DEA* will likely cause many single traders, small trading groups, and even larger commercial 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, to have to register as floor traders. This will add layers of administrative complexity to their businesses, without advancing the risk oversight, because a DCO member's oversight is already fully integrated into the available trading systems.

Proposed Reg AT also requires AT persons to maintain a source code repository. Source code in a repository could be subject to the inspection by both the CFTC and the DOJ, without subpoena or any formal opportunity by a source code owner to object to endeavor to restrict the manner or access or use of the source code. TT believes these requirements in the CFTC and DOJ's inspection authority are unnecessarily and extraordinarily broad, not likely to provide helpful information, likely amount to an unconstitutional taking of individuals' property, and are generally unnecessary to achieve the goal of the proposed regulations.

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.

Source code is also complicated, and the breadth of the relevant code might be so expansive that it is hard to fathom how it would be compiled, stored, or used effectively by the Commission. A useful example of the underlying complexity of seemingly simple commands appears in our first comment letter to the Commission. 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 in various ways, depending on many factors.

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 ensure that the code is reviewed when truly necessary.

The last issue that I want to address is the testing requirement set forth in Reg AT. TT believes that such testing should focus on the output of an algorithmic trading system, rather than the source code underlying such systems. As proposed, source code underlying an algorithmic trading system would be subject to substantial, highly prescriptive testing in advance of a system's rollout, and continually thereafter. TT's customers test algorithms every day, but the proposed language of Reg AT seems to require a registered entity to test software code 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 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.

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

[The prepared statement of Mr. Ryan follows:]

PREPARED STATEMENT OF MICHAEL G. RYAN, EXECUTIVE VICE PRESIDENT AND GENERAL COUNSEL, TRADING TECHNOLOGIES INTERNATIONAL, INC., CHICAGO, IL

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 letters¹ 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) 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.

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

(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 cus-

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.

ATTACHMENT 1

March 15, 2016

Via Electronic Submission

Mr. CHRISTOPHER J. KIRKPATRICK,
Secretary of the Commission,
Commodity Futures Trading Commission,
Washington, D.C.

Re: Proposed Rulemaking on Regulation Automated Trading (Regulation AT)

Dear Mr. Kirkpatrick:

On behalf of Trading Technologies International, Inc. ("TT"), I am submitting this letter to comment on the Proposed Rulemaking on Regulating Automated (Regulation AT), specifically with respect to the proposed definition of Direct Electronic Access and a requirement that AT Persons be required to maintain a source code repository.

I. Background of TT

TT is an independent software vendor with approximately 400 employees located in its Chicago headquarters as well as offices in most major financial centers throughout the world. TT licenses software trading solutions enabling TT's customers to trade on 45 of the world's major electronic exchanges and liquidity platforms. TT's customer base includes the largest banks, commercial firms, hedge funds, proprietary trading firms and other professional traders. TT offers many sophisticated software applications for its customers' use such as its new software as a service "TT" platform, as well as its legacy applications such as X Trader® and X Trader® Pro, X_Risk®, ADL®, Autotrader™, Autospreader® and exchange gate-

ways. TT also hosts its customer's infrastructure at facilities co-located or closely situated with exchange matching engine technology.

II. Comments on the Proposed Rules

A. New Defined Term: "Direct Electronic Access"

TT believes that the definition of "Direct Electronic Access" ("DEA") 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 ("DCO") where the pre trade and other risk controls are controlled by such member, including when a third party maintains the physical location of the systems.

As drafted, the proposed definition is unclear and does not provide sufficient guidance as to what "being routed through a separate person" that is a member of a DCO 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 has nothing to do with the goal of enhancing risk management of such orders. Control of the risk parameters is the relevant issue and the definition of DEA should be altered to make clear that where such control exists, there is no DEA.

The manner by which TT offers access to its trading system is typical of independent software vendors in the futures industry and although the methods of software distribution are diverse, a futures commission merchant ("FCM") has the ability to fully control the risk management settings in every case.¹ Currently TT offers its software and services in four distinct ways:

- (1) traditional on-site licensing;
- (2) hosted servers;
- (3) shared hosted servers; and
- (4) software as a service ("SaaS").

On-site licensing involves licensing software that the customer installs at its location. In this case the exchange gateway software that connects the software with the exchanges is installed on servers in a server closet at the customer's location and the client side software, that generates the trading screen, would be installed on the traders' workstations.

The last three methods of distribution help many FCMs achieve significant cost savings by outsourcing order routing technology to third parties without compromising on their control of risk parameters.

Where TT hosts the servers, TT effectively moves its customers' server closets into a TT managed location. In this case TT oversees the installation of all server software and maintenance of the applicable data lines and network.

The shared hosted environment is similar in that TT hosts the server software, but here end-users can easily clear trades through multiple brokers because the physical infrastructure is shared and the software enables such relationships.

The last method is as a fully hosted software as a service offering. Here the software is installed on hosted equipment and the trader interface is Internet based so there is no software installation on the workstation other than minimal code used in the browser.

In each of the last three examples (hosted, shared and SaaS) the servers on which the gateway software connects a trader to an exchange sit at a TT managed location—not at a location managed by an FCM. TT manages the technical aspects of the hardware, software and telecommunication connections while the FCM's retain complete control over user set-up and risk management tools that are provided as part of the TT order entry systems.

The current definition of DEA doesn't appear to fully recognize the relationship with such third party providers and should be clarified to allow for these common situations. 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 FCMs ability to control risk and therefore the legitimate goal of the new regulation would still be achieved.

As drafted, 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 who hedge on futures exchanges, all of whom trade through FCMs and are often substantial liquidity providers. This will add layers of administrative com-

¹ Some FCMs choose not to utilize TT's risk controls and instead rely on exchange provided risk tools, but the FCM may always control risk through the TT system if it chooses to do so.

plexity to their businesses and require them to hire expensive compliance experts to their staffs. Yet, no further risk oversight would be achieved because an FCM's oversight is already fully integrated into the available trading systems. The goals of the Commission will not be achieved and the cost of compliance for these individuals and small groups will often price them out of the market.

B. Source Code Repository

TT is concerned that the requirement under section § 1.81(a), that AT Persons “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” is 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. To be clear, TT strongly urges the Commission to remove this requirement from the proposed regulation.

1. Source Code Is Highly Proprietary and Typically Not Made Available to Third-Parties

Although it is unclear exactly what is meant by the term “source code” in the proposed regulations,² TT assumes that the term source code generally means software expressed in a high-level language intended to be intelligible by humans. Except with respect to open source licensing arrangements, to our knowledge, source code is never licensed under any software license agreement offered by any software provider including any independent software vendor 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.

TT is very concerned that despite numerous protections for confidential information submitted to the CFTC, there are gaps in such protections as well as too many possibilities to escape the CFTC’s control through unintentional means such as third-party cyberattacks.³ If trade secrets⁴ are compromised, the trade secret status would likely be lost along with a firm’s economic advantage over its competitors. Such an action would likely amount to an unlawful “taking.”⁵

It is also worth noting that much of the relevant source code potentially used by AT Persons comes from third party software providers like TT and others such as Microsoft. TT offers multiple applications through which a trader could implement an algorithmic trading strategy. Yet, TT never licenses its source code and would not provide it to its customers in any circumstances. TT is not alone in this position. For example, many traders utilize commonly available tools such as Microsoft Excel® to implement their trading algorithms. They might develop the algorithm in Excel and connect Excel to a commercial trading application like TT. Based on the movement of the market and the algorithm, orders might be triggered as a result of actions implemented in Excel. TT has not contacted Microsoft, but we suspect

²TT believes this term needs to be clarified if the Commission insists on keeping this requirement. The Commission should also clarify which source code is relevant. As written, it seems the Commission is looking for a wide array of code that would touch all aspects of a trading system.

³Although TT appreciates that a party submitting information to the CFTC may request that the information be treated confidentially pursuant to the provisions of CFTC Rule 145.9, the Assistant Secretary has discretion to grant or deny requests from requestors of non-public information. Moreover, it is TT’s understanding that Congress, and other governmental authorities—both U.S. and non-U.S.—may also request non-public information, and a submitter of non-public information may not be advised of this request or outcome. Finally, despite the best protections by the CFTC, cyberattacks and other unauthorized intrusions, as well as the illegitimate actions of staff acting contrary to their legal requirements, could compromise the sanctity of non-public information submitted to the CFTC.

⁴The Uniform Trade Secrets Act (“UTSA”) defines a trade secret as:

- information, including a formula, pattern, compilation, program, device, method, technique, or process,
- that derives independent economic value, actual or potential, from not being generally known to or readily ascertainable through appropriate means by other persons who might obtain economic value from its disclosure or use; and
- is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

⁵See, *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986 (1984).

that software companies like Microsoft would not be willing to divulge their source code either.

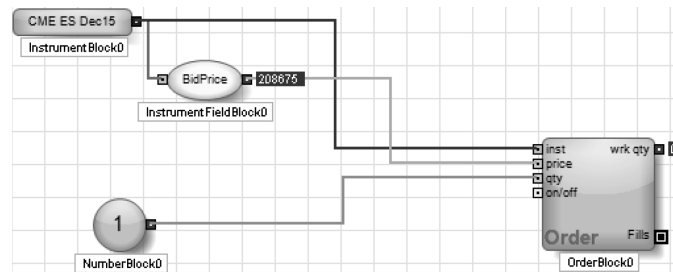
2. Source Code Is Complicated and the Potentially Relevant Amount of Source Code Is Enormous

Even if the Commission was able to overcome the legal impediments relating to forcing disclosure of trade secrets, it is doubtful that such information 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.

In the Excel example above, Excel interacts with TT software, which includes and interacts with multiple layers of applications and libraries, which interact with other layers of messaging software and other systems on down the line until the operating system is utilized. In order to recreate the intent of the algorithm through the source code, the Commission would need to compile the code in the same environment where it was set up, including the same version of each layer of code and the same version of the exchange's software. Short of that, it would likely not work the same as it was intended or as it might have worked at a moment in time. The code behind each layer of production software changes often. New releases occur regularly (often monthly) plus smaller code patches are released in between. Assuming there will always be a time lag between trading activity and when an investigation is started, the Commission would need to be able to recreate the exact version of code including revisions and interim patches of each layer of code that was in use at the point in time of the trade. Each layer of code interacts and depends on the other layers to work as planned. A single version of a single layer of such code could be millions of lines; a repository of all possible code versions going back in time for years would be much, much larger and impose an immeasurable burden on the industry.

As an example, consider the following simple algorithm that is depicted in TT's "Algo Design Lab" application:



The logic of this simple algorithm is as follows: (1) submit a limit order for the given instrument and quantity at a price equal to the bid; (2) when the bid price changes, re-price the order to be the same as the bid.

The simple image above belies the complexity and enormous amount of source code that generates this image and effects the strategy. One can imagine the image above as a depiction of the highest level of code used to effect the strategy. The strategy itself would run on a server application in the TT environment but it would also touch and be dependent upon almost every part of the TT trading system. The way that the algorithm subscribes for prices, downloads contract information, and routes orders is specific to the way that the underlying components have implemented and exposed this functionality. So technically, one would need all of the TT system software in order to *attempt* to reproduce its behavior. Hundreds of applications and libraries within the TT system itself are essential components and the source code would likely add up to millions of lines of code for the TT applications only. If the trader used Excel for the algorithm, the Microsoft code would also add millions of lines of code most likely. Add to that the many other third party applications involved in the process for price feeds, analysis, messaging, the operating sys-

tems of the workstation and the servers among other layers of code and there would be an immeasurable morass of code that, in theory, would need to be stored and made available to the Commission.

This is a very simple example. The complexity of this simple example is magnified dramatically in a more complex and realistic example, not to mention situations where multiple algorithms are in question.

3. 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 and how and when coalescing happens may vary from moment to moment depending on many factors such as network routers, firewalls, switches, server hardware, operating system, vendor software, coalescing and conflation factors. 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 multiple 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.

Consuming market data is like drinking from a fire hose. The basic process by which TT delivers market data to clients is as follows:

1. TT receives a market data update from an exchange (*e.g.*, bid price = 100).
2. TT broadcasts the update to other servers in TT's trading network.
3. The TT system notifies the client application.
4. TT receives another market data update (*e.g.*, bid price = 101). If the client has finished processing the last update, the TT system notifies the client of the update. If not, the system waits—and then delivers it when they are ready.
 - (i) While waiting, the TT system might receive thousands more updates. TT conflates this data, meaning it overwrites the values that will be delivered to them when appropriate. This is done because no one wants to receive “old” market data updates.
 - (ii) The time it takes a client to process an update depends on a variety of factors, including system load, network load and operating system scheduling. This makes it extremely difficult to determine the exact price update that the client might process to re-price the order. So even with access to identical system software, intermediate network and server infrastructure and the algorithm, one would likely be unable to reproduce the exact behavior of an algorithm for most liquid markets.

Even assuming, for the sake of argument, that the Commission could make heads or tails of 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 to every exchange and the Commission 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. Even where more is necessary, 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 truly be necessary. In fact, subpoenaing a written description of the intent of a trade or the basic algorithm that describes the strategy should be enough without even delving into source code. This would amount to a document detailing the logic of the algorithm that would direct the trade (*e.g.*, “if market price = X then enter buy order at Y.”)

The extraordinary burdens described above, the potentially illegal or overly damaging intrusion into proprietary source code incurred by trading firms and their software suppliers and the questionable benefit of obtaining any further code far outweigh any benefit from acquiring the code.

* * * * *

TT is very concerned that, as drafted, Regulation AT will not positively enhance the existing regulatory regime for automated trading. We addressed two aspects of the proposal about which independent software vendors like TT seem to have good

insight. We are more than willing to provide additional input about these matters or others matters within our expertise.

Please contact me at (312) 476-1081 if you have any questions or seek additional information.

Respectfully submitted,



MICHAEL G. RYAN,
Executive Vice President and General Counsel.

ATTACHMENT 2

June 26, 2016

Via Electronic Submission

Mr. CHRISTOPHER J. KIRKPATRICK,
Secretary of the Commission,
Commodity Futures Trading Commission,
Washington, D.C.

Re: Proposed Rulemaking on Regulation Automated Trading (Regulation AT)

Dear Mr. Kirkpatrick:

I am submitting this letter on behalf of Trading Technologies International, Inc. ("TT"), to respond to certain issues raised during the June 10, 2016 public roundtable discussion regarding Regulation AT. Specifically, TT would like to address proposed testing requirements for Algorithmic Trading (as defined in Regulation AT) systems and software.

Section 1.81 Testing Requirements Should Be Limited to Testing Finished Products

TT applauds all reasonable regulatory initiatives to ensure that market integrity is enhanced through testing of Algorithmic Trading systems and software. TT believes that Section 1.81(a) of Regulation AT, which would impose certain development and testing requirements for Algorithmic Trading systems, should be clarified so that it can be implemented in the most practical and useful manner. 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.

TT Performs Regular Tests on the Software It Licenses

As a third party software vendor, TT's view of the proposed rules may be different than entities that are directly regulated by the Commodity Futures Trading Commission ("CFTC"). TT practices commonly accepted development and testing practices and only licenses systems and software that have been subject to a rigorous testing protocol. This protocol includes:

- testing in a development environment separate from a production environment;
- back testing and stress testing;
- documenting the specifications and requirements of source code; and
- retaining of source code in an environment where changes are recorded.

TT's practices are consistent with the requirements the CFTC proposes to be adopted by AT Persons. In fact, other independent software vendors in the futures world, and most likely all companies that license software and systems, such as Microsoft, Adobe, Google, *etc.*, already follow those practices every day in an effort to produce software and systems that perform as intended.

Only Testing of the Finished Product Is Relevant to Regulation AT

As TT indicated in its previous comment letter and during the roundtable discussion on Regulation AT, in no event does TT or any software vendor in any industry provide access to source code as part of its license grant to its customers.¹ But, any software product provided by TT to any customer is always available for the customer's testing and TT expects that each customer performs appropriate testing prior to utilizing the software in production environments. In fact, TT offers testing

¹The exception to this statement would be vendors who license open source software.

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 the developer of the product.

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 "regulated" by the market for software and systems.

An important distinction between the sort of testing that clients perform every day on their third party 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 licensed. To the extent the entity licensed the product from a third party, the 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.

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 in TT's prior comment letter, several other comment letters and verbal comments to the CFTC.

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, such as Microsoft through its products like Excel[®],² licenses source code to its customers and will not willingly do so.³ 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.

Whether a Product Is Licensed from a Third-Party Does Not Change the Appropriate Testing Procedures

Some have argued that, absent a requirement by the CFTC, an FCM or other regulated entity would have no control over how third party code might be tested, monitored or altered to address issues that may arise in an algorithmic trading environments. When looked at from a practical perspective, such an objection has no merit.

If an FCM was to test an algorithmic trading system it would run the algorithm in a simulated environment to determine what the outputs of the system would be under various market scenarios. If a problem was detected by a tester or compliance specialist, that person would turn off the algorithm,⁴ contact the developer of the algorithm, point out the problem and ask the developer to fix the problem. The developer would then review the code that implemented the algorithm and make any appropriate adjustments. Then the algorithm would be retested in the simulation environment and the process might repeat itself until the algorithm was determined to be running as planned. The process would be the same if the problem was discovered in a production environment—the algorithm would be turned off and it would be fixed by the developer and then tested in a simulation environment before being used again in a production environment. If the algorithm had been developed in-house at an FCM that developer might sit down the hall from the tester or the compliance specialist. If the algorithm was developed by a third party, the developer would be a phone call away. The testing would be the same and the resolution of any issues would be the same.

* * * * *

TT, respectfully, remains very concerned that, as drafted, Regulation AT will not positively enhance the existing regulatory regime for automated trading. We appreciate the opportunities afforded to us to comment on Regulation AT and are more than willing to provide additional input about these matters or others matters within our expertise.

² Excel is a registered trademark of Microsoft Corporation.

³ As indicated in TT's original comment letter, TT has not been in contact with Microsoft, but we would suspect that commercial software companies like Microsoft would not be willing to divulge their source code.

⁴ Mandating such a kill switch seems prudent.

Please contact me at (312) 476-1081 if you have any questions or seek additional information.

Respectfully submitted,



MICHAEL G. RYAN,
Executive Vice President and General Counsel.

The CHAIRMAN. I want to thank our witnesses.

The chair would remind Members they will be recognized for questioning in order of seniority for the Members who were here at the start of the hearing. After that, Members will be recognized in order of arrival. I appreciate Members' understanding.

And with that, I will recognize myself for 5 minutes.

Mr. Wood, under the broad definitions provided in Reg AT, and the ubiquitous use of automated trading in the market, what percent of market participants do you think would qualify as AT persons?

Mr. WOOD. Thank you for the question, Mr. Chairman. We have seen an adoption of automated trading in the futures markets that has become prevalent in many ways. Reg AT has tended to focus on a particular type of participant. The argument that FIA has made is automated trading is used by a lot of different types of market participants in one form or another. There are people who use highly sophisticated systems that they develop themselves, but there are people who also increasingly use systems that are provided by software vendors or by the FCM community for them to execute more efficiently within the futures markets.

So trying to quantify how much of the market is truly algorithmic in nature, it is going to actually be a very high percentage. And I would actually defer to Andrew Vrabel here, because they use metrics on their orders going into the CME Globex platform that actually highlights whether an order is manually generated or automated.

The CHAIRMAN. Mr. Vrabel, do you have that number off the top of your head?

Mr. VRABEL. The number off the top of my head is that, in our agricultural markets, roughly 50 to 53 percent of total volume comes from automated strategies. And as I had mentioned before, every type of market participant, not every participant but every type of participant uses some form of automated trading strategy or another, whether it be, as Greg said, a highly complicated algorithm or a simple auto spreader available through any ISV or software contractor.

The CHAIRMAN. Mr. Gorelick, some would argue that the CFTC should use Reg AT to involve itself in the inner workings of algorithmic trading systems to anticipate problems. Is it remotely possible that the CFTC would be able to anticipate problems in the market by studying source code?

Mr. GORELICK. I would say it is highly implausible. I was trying to think of an analogy that would help to sort of explain what this test would be, and it is tricky for a variety of reasons but, the best I can come up with, it is sort of like taking a car apart, and taking all the pieces and studying them in excruciating detail to try and predict traffic patterns. It is sort of relevant, if you want to figure

out how to build a car it is very useful, but it is not the best way to measure traffic patterns. What you really need to do is go out there and measure. And that is what we are trying to do. By looking at source code, with millions of lines, with lots of interactions that are very dependent on the specific market data that is coming in at a particular time, that is very dependent on the hardware that it is running on, the network characteristics, it would be very difficult to determine future market events by studying source code.

The CHAIRMAN. Let me ask you, some of you mentioned this two-tiered level of pre-trade risk controls. Are there barriers to those being implemented now on a voluntary basis? Mr. Vrabel, is that scheme already in place, the two-tier that you talked about?

Mr. VRABEL. Yes, the scheme is largely already in place. The exchanges have comprehensive market integrity controls that have been in place for years. By and large, every market participant has some degree of risk controls.

The real question under Reg AT is whether those risk controls are adequate, given the scope and scale of that particular algorithmic trader. But yes, in our experience, I have not encountered a firm that has zero risk controls in place.

The CHAIRMAN. Well, I am talking about that two-tiered system that you have mentioned where, obviously, the trader should have controls in place, the FCM should have controls in place, the DCM should have controls, is there something preventing the SROs from actually requiring that to be in place already?

Mr. VRABEL. There is not, and the two-tiered model is what we have offered instead of a more complicated structure, for example, portions of Reg AT lead one to believe that there could be as many as three tiers. The exchange has to have an appropriate level, the clearing firm has to have a level of protection, and the algorithmic trader has to have a level of protection. And, redundant measures like that we not believe are——

The CHAIRMAN. Okay. The Ranking Member mentioned 15 to 30 issues a year in which that happened. Are those numbers going up or down as a result of the array of controls that self-imposed has had? Is that getting better or worse?

Mr. VRABEL. My understanding of that 15 to 30, or 15 to 20 number, wasn't an analysis of the number of malfunctions that have caused a market disruption. Instead, it was based on a calculation of markets that have had price swings of a certain degree over a period of time. One important thing to note is that the preamble to Reg AT notes significant market events resulting from algorithmic trading, and the only one in CFTC-regulated markets is the May 6, 2010, flash crash that the CFTC addresses there. And since that point in time, there have been 12 billion trades on CME's markets.

Now, obviously, we have had other small events, but the risk protections that are in place we believe are adequate, and have been adequate to address those.

The CHAIRMAN. Yes. Thank you.

The Ranking Member, 5 minutes.

Mr. PETERSON. Thank you, Mr. Chairman.

Does the Division of Market Oversight have subpoena authority? Does anybody know?

Mr. WOOD. I believe the Division of Enforcement at the CFTC does.

Mr. PETERSON. The Enforcement Division has subpoena power?

Mr. WOOD. Yes.

Mr. PETERSON. Is there a Division of Market Oversight?

Mr. WOOD. I believe in this circumstance, the various divisions at the CFTC would work together if they needed to take this course of action.

Mr. PETERSON. I guess, as with a lot of the stuff that we found out as we went through all of this that until you get into enforcement, sometimes you can't find out anything about what is going on with these things, unless you get into an enforcement situation. Is that right?

Mr. WOOD. I believe so, yes.

Mr. GORELICK. Ranking Member Peterson, that is a good question. What I have suggested is that the best way to figure out what is going on with an algorithm or with a particular trading strategy is to really look at the data, at the orders and the fills and the cancellations, and all of the audit trail information that is readily available to the exchanges and to the CFTC. That is going to give you a much better idea of what is going on with the trading strategy than sort of a preemptive, extraordinary code review.

Mr. PETERSON. Well, can they get that information?

Mr. GORELICK. Absolutely. I think that is where ongoing investment is warranted. Right now, one of the great advantages of electronic trading and of the electronification of our markets has been that there is now a complete audit trail available of every message that is sent back and forth from the exchange by traders and everywhere else. And that allows sort of an unprecedented level of transparency into what is going on in the markets. Regulators need to continue to develop their skills and their technologies and their toolsets to conduct that analysis, but right now the exchanges already have terrific surveillance capability built on these audit trails, and the CFTC has an opportunity to piggyback on that as well.

Mr. PETERSON. Yes. So they don't have enough resources to do as much of this as they should, is that—

Mr. GORELICK. Yes, I am not sure, this is something that has come up at the Technology Advisory Committee over the years. I think that is really more of an issue for Congress and for the CFTC to talk about resource-wise. I certainly think that it is an area of focus to make sure that they are investing appropriately in both their technology and in their analytical capabilities. I think that is going to be a much better, more efficient investment than in source code review capabilities.

Mr. PETERSON. Are they doing that?

Mr. GORELICK. I believe they are, yes. Whether it is enough, whether it is sufficient, whether they could do it better I am not positive about.

Mr. PETERSON. Yes, with a lot of these different issues, it seems like people get more tied up in all the enforcement stuff and they miss the trees for the forest. When I was on the Intelligence Com-

mittee, I had a similar issue with the FBI, who were not doing what they should be doing, because they were more worried about enforcement than they were trying to figure out what was going on. Do you think that the CFTC has figured this out and is moving in the right direction?

Mr. GORELICK. I would say that they are moving in the right direction. This has clearly been an area of focus and a lot of discussion at the Technology Advisory Committee. I do think though that this is an area that probably needs more focus. It would be a more fruitful avenue to pursue than the source code provisions in Reg AT.

Mr. PETERSON. Yes, sir.

Mr. RYAN. If I may add something. One thing that I want to note is that I have been at TT for about 17 years, and we often get contacted by the CFTC, sometimes the Department of Justice in an enforcement action and the like, and asked questions about our technology. The questions are how does it work, can you give us some documentation to explain how it works in this scenario or that scenario. And we are always there to answer those questions. We are always happy to do that. But never once in my 17 years at TT have we ever been required to provide source code.

So it just seems to me, the source code avenue is an avenue that is not likely to help in this analysis.

Mr. PETERSON. Well, Mr. Chairman, maybe the Committee should look into that and find out more about it.

The CHAIRMAN. Well, I do think the proprietary source code, the property-taking under the Constitution, they are troubling that they can simply request that. It is apparently on everybody's mind.

Do you yield back?

Mr. PETERSON. Yes.

The CHAIRMAN. The gentleman yields back.

Mr. Goodlatte, 5 minutes.

Mr. GOODLATTE. Mr. Chairman, thank you for holding this important hearing. And thank you to the panel for being with us today.

While there may be a number of significant concerns with this rule, I would like to zero-in on one particular aspect that has been mentioned several times already today in this issue of source code repository.

It seems that through this rule, the CFTC has decided to use its legitimate authority to access books and records as a means to illegitimately force trading companies to turn over valuable intellectual property without first obtaining a subpoena. And I am disturbed by this decision and, therefore, I have a few questions for the panel.

First, how difficult is it currently for the CFTC to obtain a subpoena for a source code, and who at the CFTC can authorize that type of action? Anybody answer that? None of you know?

Mr. Vrabel.

Mr. VRABEL. I am by no means an expert on the administrative procedures, but my understanding is that an administrative subpoena has to be approved by all Commissioners.

Mr. GOODLATTE. All the Commissioners, right. But nonetheless, if they have a desire to subpoena documents from any of the companies that are affected by this, they have the ability to do that.

Second, how will this type of unfettered access to source code be beneficial to the CFTC? Would this reduce risk to the system, or does CFTC currently retain staff able to easily understand and interpret the code? Mr. Gorelick, you have commented on this a bit already. Could you elaborate on that?

Mr. GORELICK. I did. No, I don't think the CFTC has the capability to routinely evaluate large amounts of source code. The software programs are written in lots of different programming languages, they are very extensive, they are often—really the best way to understand exactly the inner workings is to talk to the software developers involved in writing that code.

As I referenced, I think it would take an army of software developer regulators, and I am pretty sure that the CFTC does not presently have that capability.

On a one-off basis in connection with an enforcement action with a very narrow set of actions, it may be useful. And I am not aware of any circumstances in which the CFTC thought they needed source code for that purpose and were unable to get a subpoena. What we are really talking about is a due process concern. The times in which the CFTC would need to access source code, they can get a subpoena, they can use the subpoena process, and there will be adequate protections built in.

Mr. GOODLATTE. We are also talking about a security concern here, aren't we? I mean isn't this something similar to the Apple-FBI dispute where the FBI wanted to compel Apple to unlock something? Here, they are asking for the authority to have automatic access to it, and once they have automatic access to your source code, what are the risks involved that it will fall into the wrong hands; either a competitor or a criminal, or even a foreign government that might use it to manipulate the market?

Mr. GORELICK. Firms like ours, firms that use automation in the markets, generally hold their source code to be very important to their business. They take their own precautions to protect their source code. They store it in secure ways, they secure their network, they have the cybersecurity defenses, they have authority about who is allowed to access it and under what circumstances. Once it is out of a particular firm and in the hands of sort of any third party, the firm loses the ability to manage those controls. And as we have seen, there is risk that if the information is attacked by third parties in some type of a cybersecurity attack, or simply that information gets out there. People change jobs, it moves from one place to another, and it could really have a negative impact from a competitive standpoint. So generally, the issue is who is able to have the types of controls that are required.

Mr. GOODLATTE. Right, and it exponentially could increase the vulnerability of that source code to discovery by individuals who shouldn't have access to it. You have to worry about yourself. Businesses are hacked all the time.

Mr. GORELICK. Right.

Mr. GOODLATTE. Government agencies, retailers, credit card companies, the list goes on and on of people who have had important

information hacked, including, in some instances, their very source codes. So if this is in the hands of a government agency, that wouldn't inspire your confidence that your vital piece of how your business operates will be better protected. It will be more vulnerable, will it not?

Mr. GORELICK. I think that is the case whenever it is outside of our hands. A government agency would just be like any other third party from that regard that we don't control who is able to look at this information, how they are able to get it, what security they have put in place. We only like to have a very small group of people inside our firm who are responsible for those controls, and not more broadly open access.

Mr. GOODLATTE. Thank you very much.

Thank you, Mr. Chairman.

The CHAIRMAN. The gentleman yields back.

Mr. Scott, 5 minutes.

Mr. DAVID SCOTT of Georgia. Thank you, Mr. Chairman.

I certainly applaud the CFTC's overarching efforts to bring the futures markets' regulatory regime into the 21st century. And as a matter of fact, it was almost a year ago to the day, in July 2015, that the Chicago Mercantile Exchange, CME, shuttered the last of its trading pits after 167 years of operation. So it makes a great deal of sense that the CFTC move on these rules now that trading pits are officially a thing of the past. However, when I heard that the CFTC would require people affected by this rule to not only retain all copies of their source code, but also make it available to the CFTC at their demand, without a subpoena. It caused me great alarm.

So I wanted to first ask the panelists if each of you drew the same conclusion that I have, in that the Reg AT being unprecedented, and that it could demand source code without a subpoena. Everybody agree?

Mr. RYAN. Yes, I will address that first, if I may, Congressman.

From our perspective, TT and the others in the industry are always willing and able to help with useful information, when that useful information is available. The biggest concern, in addition to the security aspect of handing over the source code, is that it is unlikely that in any scenario it is actually going to be useful. I gave an example on one of the comment letters that I issued to the CFTC that had an image of a very simple algorithm. It was just an image where you entered an order at the best bid on the market, and if it moved, you went with it. It is an image that is maybe about this big.

Mr. DAVID SCOTT of Georgia. Yes.

Mr. RYAN. Okay. The amount of code that goes into generating that image and then executing the order that that image tries to put into place is incredibly expansive. I mean we are talking like millions of lines of code, ultimately, to effect that simple of a process.

Mr. DAVID SCOTT of Georgia. And let me get rather specific here for a moment. And, Mr. Vrabel and Mr. Gorelick, you touched on some of this, but do you think that the CFTC should have a definition of *automated trading* that separates out automated execution from algorithmic strategies that drive trading decisions? My worry

stems from the CFTC forcing automated traders to share their algorithmic strategies or secret recipes with the CFTC, whenever the CFTC wants it. Now, couldn't a better solution to this problem be that if the CFTC separated out those two definitions, we could better protect these secret recipes?

Mr. VRABEL. Respectfully, Congressman, I don't know if that will adequately address the issues. In my experience when our teams have reviewed and monitored disruptions in the markets resulting from automated trading, algorithmic trading, or simple devices like order routers, we see as many malfunctions that cause disruptions in the markets from very simple devices as we do from highly complex ones.

Mr. DAVID SCOTT of Georgia. Yes.

Mr. VRABEL. So from my perspective, if there is going to be risk controls that are addressing automated trading, it would need to include the algorithmic, highly complex, and the very simple order routing automated strategies.

Mr. DAVID SCOTT of Georgia. All right, and determining the boundaries of a particular group of market participants is always a problem when trying to define the scope of regulation. I serve on the Financial Services Committee, and we have that problem all the time. But oftentimes we deal with this problem by regulating the activity that is being done, as opposed to regulating the entity that does it.

I wonder if we are encountering a similar type of problem here with the definition of the *AT person*. Is the scope of this regulation exhaustive, are the lines we are drawing with this *AT person* definition too big, is it too small, and could a better way be to regulate the activity that the *AT person* is doing as opposed to regulating the entity?

Mr. WOOD. Congressman, if I can take that one. FIA has certainly always advocated that there shouldn't be a very strict definition of who is an *AT person*, because the lines have increasingly become blurred between automated and algorithmic trading to the point that it becomes meaningless in the sense of the interaction with the marketplace. And to your point, we have stressed to the Commission that they should be looking more at the what, the actual activity, the automated nature of the activity in the U.S. futures markets, as opposed to trying to look at the who, and trying to create some sort of arbitrary categorization where people either fit into that category or outside of that category, which really doesn't do anything to protect the overall integrity of the marketplace.

Mr. DAVID SCOTT of Georgia. Okay. Thank you, sir.

Thank you, Mr. Chairman.

The CHAIRMAN. The gentleman yields back.

Mr. Lucas, 5 minutes.

Mr. LUCAS. Thank you, Mr. Chairman. And thank you to the panel for being here today.

A big part of what we do is establish a base of information and knowledge, in these Committee hearings. So just go back to the fundamentals for just a moment, and I would say, Mr. Woods or Mr. Gorelick, or whoever would like to answer this question, explain to us for just a moment what the benefits of automated trad-

ing provide to the participants, that fundamental question about why this matters. Surely it benefits someone or we wouldn't be doing it, right?

Mr. GORELICK. Absolutely. If you look back at the development of the markets over the last 15, 20 years, as markets have become more electronic, market participants have started to automate a lot of the functions that they did previously. So in terms of evaluating market data and what is going on, in terms of placing orders, in terms of adjusting orders, in terms of managing risk, all of those functions are, in many ways, better handled by a computer much more efficiently than they were able to be handled previously. And the result of all of that is that costs for end-users in the markets have come down. And if you look at the data, sort of end-user costs in a variety of markets that have become increasingly electronic, increasingly automated, and in turn, increasingly competitive, the result is that the costs to the end-user are much lower. And that is the primary benefit of automation.

Mr. LUCAS. Increased efficiency of the process. Absolutely.

Mr. Ryan, in Reg AT it doesn't appear to provide a real definition of what *source code* is. Is there some universal definition that CFTC and other entities like to use?

Mr. RYAN. Yes.

Mr. LUCAS. Because we have come a long ways in my 40 years from playing with COBOL and FORTRAN in those freshman classes back in the 1970s.

Mr. RYAN. Sure. I don't think that the general definition of *source code*, first, I don't think it is really defined in the proposed regulation, but I don't think that is too controversial a concept. Basically, it is a high-level software language that is supposed to be written in a way that is intelligible to humans. So it is not the machine language, it is not binary code. The part that is more concerning is the breadth of the source code that is being requested under the regulations.

Mr. LUCAS. One last question. Mention was made about not just proprietary code developed by a firm, but vendors being available to purchase this from. For curiosity's sake, how much of an industry is this, do we have dozens or hundreds of vendors who have these products for sale, retail?

Mr. RYAN. Well, we have—

Mr. LUCAS. And I address that to anyone who would care to respond.

Mr. RYAN. Sure. I mean, actually, others might know it better than I do, but we have many. I mean I would say in the futures worlds, maybe a dozen or more, or dozens, I guess, vendors that are available.

Mr. WOOD. Yes, I would add from an FCM perspective where we provide access to our customers, we see many firms who either write their own code or are using third parties, or they are even using algorithmic trading software provided by ourselves. And in terms of numbers, there are, yes, certainly many different types of firms that provide different levels of type of automation.

Mr. LUCAS. And with the resources involved and the sophistication of the users, I would assume this is an incredibly competitive

process developing this software for sale, and I can just imagine how competitive.

With that, Mr. Chairman, I yield back.

The CHAIRMAN. The gentleman yields back.

Ms. DelBene, 5 minutes.

Ms. DELBENE. Thank you, Mr. Chairman. And thanks to all of you for spending time with us this morning.

Everyone has brought up the issue of source code and concerns about unfettered access to source code, and not maintaining a subpoena standard. Mr. Ryan, brought up the issue of kind of the access of code with actual data flows coming in. And when you are doing testing and there are obviously the requirements on testing within the regulation, can you talk about how you develop code and how you test it, test your source with data so that you can understand how it is working?

Mr. RYAN. To a degree, I can talk about that. I am the lawyer, I am not the technologist.

But yes, throughout the development cycle we test the data to look at things like how it is working functionally, whether there are security issues involved with it, whether the code is written appropriately, how it works in relation to the market itself. An issue that I have raised on this is that I question whether that review of code is really the relevant test, as opposed to the review of the output of the product because it is that output that is really what is relevant to an analysis of whether there is a problem, at the end of the day.

Ms. DELBENE. Do others have feedback on how you test and how you combine those two together to one, see if you are getting the results that you want in terms of creating the product that you thought you were creating?

Mr. GORELICK. Well, that is a very important point that the software in and of itself won't tell you very much about what is going to happen in the market. It is really an issue of seeing how the software runs in a live market.

Now, what we do internally is lots of different kinds of testing. We do component-level testing where we look at a particular piece of code and develop test cases around that to make sure it is functionally the way we intend. We do system-level testing where we actually dummy-up information sources so that the information comes, in a way that is as close to what we expect to see in the real market as we can. And then we do live-market testing where we actually trade these markets, after they have passed all of our other tests, at small scale in the market to make sure that they do what we expect them to do, based on all of our testing.

There is extensive testing that goes on. The real core of the issue is though, from a software standpoint, is looking at the software close to enough to let you know how it is going to operate in the real live market, and when you are not taking into account all the data, the timing issues, the hardware issues, the network issues, it is hard to get comfortable that there will be a lot of insight gained from that.

Ms. DELBENE. Yes.

Mr. WOOD. And if I can just add to that. Source code is the basis for when something is actually running in production. There are a

lot of runtime parameters; *i.e.*, real-time inputs, that come not just from the people who are using the software, but also from the market itself. And these are factors that, obviously, influence how the software then interacts with the market. Generally, across the industry, we have been trying to say the only way that you can try and control this is to ensure there are appropriate pre-trade risk controls in place to mitigate the possibility that something may go wrong, or something may occur that could disrupt trading in the marketplace.

Ms. DELBENE. All of you are saying if you aren't really studying the overall environment, just looking at code and looking at the lines of code, you are not necessarily going to have the insight you would have unless you saw the entire environment, which is the data flowing through the system and the output of the system, which I guess speaks to the point that you made, Mr. Gorelick, earlier about the resources that would be required there.

Secondarily, then there is the protection, the protection of source code and trade secrets and IP, and does anyone have any problems with the way things have worked to date in terms of having the subpoena standard that has been in place?

Mr. WOOD. One thing I would just say to that is it usually takes several steps before it gets to a subpoena level. Working for an FCM, we often get inquiries from both the SROs and from the CFTC for a section 4g inquiry where they are asking for information. And, of course, we will try our best to provide that information. We will talk to our customers if it involves their customers, if they are direct members of the SRO, obviously, they would be directly approached. So we would go through all appropriate steps to provide as much information and background before we got to the subpoena process.

Ms. DELBENE. Thank you so much.

My time has expired. I yield back, Mr. Chairman.

The CHAIRMAN. The gentlelady yields back.

Mr. King, 5 minutes.

Mr. KING. Thank you, Mr. Chairman. And I thank the witnesses for your testimony.

I turn first to Mr. Gorelick, and I pose a question this way. All the things we are talking about here with algorithmic trading, could you paint for us, since you have been really good metaphorically so far, worst case scenario, if we did nothing and let this thing just race where would it go, what would be the worst case scenario?

Mr. GORELICK. Markets certainly have experienced disruption, and there has been manipulation. There has really never been a market in the history that has not had some kind of problems with it, and some of those problems have come forward as the markets have been electrified and automated.

My sense is that there are a lot of safeguards that the industry has already put in place to really mitigate the risk of the worst case scenarios that we are talking about; markets spinning out of control in some way, that there are multiple layers of risk controls, there are best practices that have been discussed widely, there are audit functions from the exchanges, there are lots of things that have gone on over the years to help create and innovate multiple

layers of risk controls to help keep the market in line, and by and large, they work extremely well. Our job here today is to think about those worst case scenarios, and think about the events in which in which things have gone wrong, but it is important to note that almost all day, every day, markets trade and function extremely well.

So my sense is that, generally speaking, the worst case scenarios are largely mitigated, but we need to keep after it. We need to improve our data analysis skills from the regulatory standpoint, we need to continue to invest in technology, and we need to continue to develop best practices in a flexible regulatory environment.

Mr. KING. I tend to agree with you about the corrections that would take place along the way, but what about worst case?

Mr. GORELICK. Right. I think the worst case—

Mr. KING. How would that come about?

Mr. GORELICK. Yes, sure. What we are all worried about is market disruption such as the flash crash where the market went down very quickly and then recovered very quickly, without a lot seeming to happen to explain that quick turnaround.

Mr. KING. Okay, let me dial this back to the 2007 or 2008, the broader financial market near-collapse that we had, and the invention of the concept of too big to be allowed to fail. And if I recall, the insurance component of that was AIG, who went clear to the bottom. But there were people buying that on the way down, or there wouldn't have been a market, and those folks that bought it all the way to the bottom made a lot of money coming back the other way. So I might paint that as a worst case scenario with regard to those markets. Is there a similar scenario that you could paint with regard to the algorithmic trading?

Mr. GORELICK. Yes, that would be the concern, again, that market prices don't reflect real market realities. And typically speaking, there are so many firms looking at these markets and trading for those opportunities that, if things are working well, it pushes everything back in line. But if you have markets that are trading away from fair value for extended periods of time, that is a market malfunction, and for most people it is probably an opportunity for others. And that is an important way to think about it.

Mr. KING. And would you say that the more experience and history we have with these market fluctuations, the fewer fluctuations we have, because you would have more traders that would identify it earlier, and those corrections would come into place naturally and more quickly?

Mr. GORELICK. Absolutely. And one of the good things about the market changes that we have seen in this automated market is we are no longer just relying on several dozens of traders in a trading pit to be able to provide all that liquidity. We have the opportunity for people from all around the country and all around the world to look at this data on a level playing field, and try and push the markets back in place. I think that has resulted in fairer markets with better pricing and more liquidity.

Mr. KING. All in real-time, which they don't conceive of that in those Marxist countries.

I turn to Mr. Vrabel, and would you agree there is natural market corrections?

Mr. VRABEL. I do, and I see it. Part of my team structure is to review market events. We have reviewed every event from the flash crash through the recent market turmoil with Brexit, and we see corrective activity from participants. An example is if we look at August 24, 2015, when the Chinese equity market crashed, which led to a precipitous decline in our markets, we saw vastly different market activity than we did during the Brexit days. And a lot of this, I believe, based on having talked to firms, is that they learned from the market event of August 24, they learned from the Treasury flash crash of October 15 how to adjust to the market.

Mr. KING. And quickly, I ask you, do you believe that our traders are adequately collateralized?

Mr. VRABEL. That the traders are adequately capitalized?

Mr. KING. Collateralized.

Mr. VRABEL. Collateralized.

Mr. KING. Yes. Do they have their collateral underneath their trades adequately?

Mr. VRABEL. Yes. And we have controls in place from our clearinghouse structure, we have tools in place that allow firms to set capital limitations or risk limitations. So yes, I do believe so.

Mr. KING. Thank you very much. I thank all the witnesses.

I yield back the balance of my time.

The CHAIRMAN. The gentleman's time has expired.

Ms. Adams, 5 minutes.

Ms. ADAMS. Thank you, Mr. Chairman, Ranking Member Peterson. And thank you, gentlemen.

High-frequency trading has certainly taken off quite a bit, and it is taking the trading industry by storm, with mixed results. While it is clear that the technology used in our financial markets is constantly evolving, we must be cautious and make sure that there are standards in place to regulate these new technologies. Obviously, Reg AT seeks to provide a regulatory regime for market participants that engage in high-frequency trading, but what about the companies that only write trading algorithms and sell them to market participants? They are not market participants, but service providers to market participants, and yet you can imagine that if one of the algorithms they provided is faulty in some way, this could cause or contribute to a market disruption.

Mr. Ryan, what would be the best way to monitor or regulate third-parties who provide the technology, but do not trade?

Mr. RYAN. Well, thank you for the question, Congresswoman. It is an interesting one.

TT is generally not the type of entity that you are talking about. Although we offer some algorithmic trading tools, for the most part, we enable our customers to utilize their own algorithms onto our systems, or using our systems.

Having said that, I believe that the answer to your question is that the algorithms that are provided by third parties can be tested by the traders and by the registered entities as products to see how they work in the market, and to see whether the intended effect actually happens. That is something that can be done today, and that is the appropriate way to test those types of tools.

Mr. WOOD. If I may just add to that.

Ms. ADAMS. Yes.

Mr. WOOD. The FMCs have a responsibility in providing access to the U.S. futures markets. We talk to customers who are using different types of software, and obviously, everyone has a responsibility to ensure what they are using to interact with the market is appropriate and has been tested. And obviously, a software provider has a similar responsibility to ensure that their software has been adequately tested. However, when it comes to being used in the marketplace, it comes, again, back to these real-time parameters that are used around the software. And we in the FCM community will have many conversations with our clients about the types of software they use, the types of market access they want to use, and the types of risk controls that should be put in place appropriately. And to the previous question around collateralization of clients, the types of risk controls that we agree to put in place with our clients are based on a risk assessment of the client, and they will then act as a speed bump in situations where there may be overtrading. Now, overtrading may be deliberate or it may be accidental through the way an algorithmic trading system or automated trading system is using, but again, it comes back to the fact that we have to have risk controls in place to minimize any possibility that something may go wrong.

Ms. ADAMS. Thank you. Several comments submitted during the comment period for Reg AT suggest that a lot of the definitions included in the proposed regulation are overly broad, particularly with regard to the definitions of an *AT person*, *algorithmic trading*, and *floor trader*. So what do you believe, and anybody can answer this, is the best way to set those definitions, and what are some of the challenges in drawing those lines, and should it be based on speed or on the way a market participant enters orders?

Mr. GORELICK. There are a lot of concerns with the definitions that have been expressed and kicked around. One of the opportunities that we have, if the goal is to improve market integrity and sort of relatively quickly, is to not worry about defining classes of participants with great detail because everyone will have different opinions on what the right definition is and who should be covered by what, but rather focus on making sure that there are risk controls on every order that goes into the market.

So if we do that, we don't need to focus on some of these boundary questions, and instead just worry about appropriate risk controls at every level of the process for all electronic orders.

Mr. WOOD. And if I can just add to that. One of the challenges with trying to create some sort of arbitrary boundary, as Richard said, and we have seen this in Europe as well where people have tried to create definitions of *high-frequency trading*, I was part of the CFTC Technology Advisory Committee, along with Richard, where we were trying to come up with a definition of *high-frequency trading*, and we decided we would not come up with a definition because, first, it would be very broad, and it is a mechanism, not necessarily a style of trading, but also it creates a situation where you can almost arbitrage the situation by saying if I don't meet the metrics that have been set as the boundary, therefore, I do not have to comply with this categorization.

Ms. ADAMS. Thank you. I am out of time. Mr. Chairman, thank you, I yield back.

The CHAIRMAN. The gentlelady's time has expired.

Mr. Crawford, 5 minutes.

Mr. CRAWFORD. Thank you, Mr. Chairman. I thank the gentlemen for being here today.

Mr. Gorelick, in 1992, Congress required the registration of floor traders to prevent felons from participating in the commodities markets. Today, the CFTC is attempting to use that same floor trader registration requirement to regulate the activities of proprietary trading firms, most of whom would qualify as floor traders under Reg AT. Is there any harm in stretching the definition of *floor trader* to encompass those market participants?

Mr. GORELICK. I am thinking about it from is there any benefit in doing that. I am sort of taking the flipside of that question because I don't think it is necessary to create a new registration category in order to accomplish the Commission's risk management objectives. So I would start off by sort of questioning the benefit that is sought to be achieved with that new categorization. I would also say there are some obvious awkwardness around trying to shoehorn a group of market participants into an old definition. The old definition, for example, was geared towards individuals standing on a trading floor, as opposed to a firm.

Mr. CRAWFORD. Yes.

Mr. GORELICK. And there would be a lot of things that need to be smoothed out. What I have suggested is that it would make more sense to consider the registration requirements separately from the risk management components here, so that the Commission could figure out what the right categorizations might be, who they are trying to capture. More importantly, what are the benefits that they seek to achieve through that registration.

Mr. CRAWFORD. What is your primary objection to the agency's definition of *direct electronic access*?

Mr. GORELICK. Yes, I have not questioned the details of the definition as much as the need for that definition, again. If we are putting risk controls on all electronic orders, the question of exactly the mode in which someone connects to the market becomes irrelevant and unimportant. We can just make sure then that we have the appropriate levels and layers of risk controls, regardless of the method of access.

Mr. CRAWFORD. And, Mr. Ryan, the same question to you.

Mr. RYAN. Yes, I mean I agree with what Mr. Gorelick just indicated. However, I will also add that we have raised concerns because we definitely have individual end-users who, for example, trade on their own account. And I actually had a conversation with a guy a couple of months ago about this. He told me about the way that he trades. He trades on his own account, he happens to share space with a bunch of other people who do the same thing. They share algorithms that they wrote in Excel, and they will use those algorithms throughout the day. They trade through an FCM whose infrastructure is hosted at one of TT's facilities. The way that *DEA* is currently defined, that individual would have to register as a floor trader, arguably, because he is accessing the market through a system that isn't physically hosted by the registered agent or the registered FCM. And so I think that is problematic.

Mr. CRAWFORD. Okay. Mr. Gorelick, back to you. If an entity is required to be registered as a floor trader, what CFTC regulatory requirements would be imposed on them beyond those specified in Reg AT?

Mr. GORELICK. Actually, I am not sure about that. I would be happy to look that up. I focus more on what are the requirements within Reg AT.

Mr. CRAWFORD. Yes.

Mr. GORELICK. I am not familiar with the floor trader requirements in any great detail.

Mr. CRAWFORD. Okay. Mr. Wood, do you have anything that you could add?

Mr. WOOD. With regards to the responsibilities of being a floor trader, I apologize, not really. The one thing I would say on DEA, what we have questioned, again, because it brings into scope a lot more participants than was originally intended in Reg AT, we have generally questioned its need because it becomes almost like an arbitrary trigger again in terms of creating a requirement around someone who has a particular type of market access, which then they don't have to do if they then use a different type of market access by going through pipes provided by an FCM. And we think that it comes back to we should be looking more at what is the type of activity, as opposed to the mode of access to the market.

Mr. CRAWFORD. Okay. Mr. Ryan, did you have anything you want to add on that?

Mr. RYAN. Well, I guess just to add to what I was saying before, the significance of having that individual that I was talking about trade through an FCM is that the FCM controls his risk already, and that is the key, it seems to me, not necessarily where the physical trade is entered or how it is entered.

Mr. CRAWFORD. Okay. Mr. Vrabel, in the last 13 seconds, any comments?

Mr. VRABEL. No, I can agree with what was said. The key issue for us is where the risk controls are being administered, either by the clearing member firm that has the ability to administer those controls, or if it is by the trading firm themselves that have created their own tools, and that is really where the line comes when looking at whether those controls are adequate and who is responsible for them.

Mr. CRAWFORD. Thank you. I yield back.

The CHAIRMAN. The gentleman's time has expired.

Mr. Walz, 5 minutes. No questions?

Austin Scott, 5 minutes.

Mr. AUSTIN SCOTT of Georgia. Thank you, Mr. Chairman.

Mr. Gorelick and Mr. Wood, when Chairman Massad appeared before the Committee in February, I questioned him regarding the source code provisions in Reg AT, and his testimony was that the CFTC would only access source code using proper procedures. And why isn't a subpoena the proper procedure to get highly sensitive information like source code?

Mr. WOOD. We would all argue that the subpoena is the appropriate legal procedure for accessing intellectual property. As I said previously, it is an extreme situation though. There are other

methods to find out more information if there is a particular inquiry without going to the subpoena level.

Mr. GORELICK. I was reassured by Chairman Massad's comments in that regard that they would be open to looking at what the appropriate safeguards are, and I would suggest that the subpoena process, as it has currently been in place, is probably the best place to start.

Mr. AUSTIN SCOTT of Georgia. Well, let me ask you this then, with the breaches and other things that we have had, and the government pledge to look after your source codes, how much comfort does that give you that the government would be in possession of it and looking after it?

Mr. GORELICK. The assurances, at the end of the day, would need to go beyond just merely we are going to take care of you, don't worry about it. I think that there are lots of different types of safeguards that can go in place around sensitive information, about who is able to look at the information and in what form they are able to access the information, what are the various levels of access printed copies *versus* connected to the Internet, *et cetera, et cetera*, that would need to be thought through and put in place to give comfort in that regard.

Mr. AUSTIN SCOTT of Georgia. Mr. Ryan, could you speak to the definition of *source code* and whether or not there is a universal definition, and specifically to Reg AT, if they have been clear about what the definition of *source code* is?

Mr. RYAN. Sure. I mean as I indicated before, I don't think that the general definition of *source code* is too controversial. Very generally, as I said, it is a high-level software language that is intended to be intelligible to humans.

Mr. AUSTIN SCOTT of Georgia. Is it all written in the same computer language?

Mr. RYAN. No. No. There are many, many different languages. In fact, TT uses in excess of 30 different languages.

Mr. AUSTIN SCOTT of Georgia. Is it easy to interpret? I would assume that it is not if you use that many different languages.

Mr. RYAN. Absolutely. No, it is not. It is not. It is not even easy to interpret when you are talking to different software engineers who are working with the same sort of language. One software engineer's source code might not be very obvious to another software engineer's source code. In fact, that is typical.

Mr. AUSTIN SCOTT of Georgia. So then how would an agency maintain a staff that could actually use the information and derive anything that they may need out of the information?

Mr. RYAN. I appreciate your question, and I think that would be very difficult for them to do. And again, I think that the participants in the marketplace are willing and able to give as much useful information as we can, but there is definitely a question as to whether this sort of information is useful.

Mr. AUSTIN SCOTT of Georgia. Well, I don't have any further questions, Mr. Chairman, most of the ones that I had have already been asked, but thank you for having this hearing. And, gentlemen, thank you for being here.

And with that, I yield the remainder of my time.

The CHAIRMAN. The gentleman yields back. I also thank him for his chairmanship of the Subcommittee that has direct oversight on this.

Mr. Thompson, 5 minutes.

Mr. THOMPSON. Thank you, Mr. Chairman. Thanks to the members of the panel.

Mr. Ryan, my first question is for you. Can you share some additional detail about how commercial market participants utilize the tools that your platform provides?

Mr. RYAN. Sure. We have many different trading tools that people can use, specifically with respect to algorithmic trading, to input their algorithms. For example, we have a tool called ADL, or Algo Design Lab, which enables an individual to basically drag and drop icons onto a user interface to create kind of a logic tree that ultimately creates an algorithmic trading strategy.

We also have other tools that enable people to input algorithms or equations into the different cells on a user interface that, again, would enable them to use the algorithmic trading. It also integrates with things like Excel. Lots of our traders use Excel and integrate it into our software, Microsoft Excel. And otherwise through APIs, they can integrate their algorithmic trading strategies through our software.

Mr. THOMPSON. Sounds like many of your strategies and tools are pretty consumer-friendly in terms of, I don't want to say algorithms for dummies, but maybe a kind of thing I could actually handle. I am not sure when you are talking about dropping icons.

Mr. RYAN. ADL is one that we are particularly proud of, and the idea of it is that it enables regular traders, so to say, to be able to input algorithms without having to hire a software engineer to do it for them.

Mr. THOMPSON. Yes. Market access. What would be the ramifications for your clients if they were subject to the Reg AT simply because they used your platform to execute their trades?

Mr. RYAN. Well, I mean we have touched on some of the bigger concerns such as the source code repository. An example is that end-user that I was talking about before. When I was talking to him, he had told me that when he trades throughout the day, he will have a list of maybe ten different algorithms that he and his trading partners might use. They will be tweaking them throughout the day too, depending on market conditions.

As written, that individual trader would have to keep track of all of those changes, all of the source code related to those changes, indicate how and when that was done, and have that available for review by the CFTC, again, without subpoena power, which is a tough task.

Mr. THOMPSON. Well, thank you.

For the rest of the panel, why would imposing risk controls on market participants, instead of registration requirements, be a better means by which to regulate automated trading?

Mr. VRABEL. I will address it in part with some of my earlier comments that some of the disruptive activity we have seen in our markets have come from fairly simply automated strategies that would not necessarily be caught in how Reg AT is currently written. By participants that do not have direct electronic access, who

are nevertheless operating a simple automated strategy in the markets. And they pose similar risks to the marketplace like some of the more sophisticated firms.

Obviously, I think that everyone up here shares the same perspective that we need to protect the entire market, not just a particular subset of traders that would be burdened with these requirements.

Mr. WOOD. And if I may add to that. So when FCMs provide access to their customers, to the marketplace, we have discussions with the clients about what sort of systems they are using, what types of controls they have in place. And if they choose to bypass the systems that we provide for market access, where we have risk controls that we administer, and they choose to use either a third-party software which may or may not give the FCM the ability to set those risk controls, then if they are going direct to market without something the FCM can provide, then they have a responsibility to ensure that there are appropriate risk controls in place.

The industry has generally taken that approach that there is this responsibility. The Commission feels that they have to go one step further with regards to then saying, "Okay, if you are not going through an existing registrant, you should become registered, and in this case it would be as a floor trader, because of the type of access you have."

We have generally argued within the industry that is probably going a little bit too far, though we have conceded that if someone chooses not to go through the risk controls provided by an existing registrant, such as an FCM, then, okay, they will become registered in themselves.

Mr. THOMPSON. Yes. Thank you, gentleman.

Thank you, Mr. Chairman.

The CHAIRMAN. The gentleman's time has expired.

Mr. Allen, 5 minutes. Rick.

Mr. ALLEN. Yes, sir. Thank you, Mr. Chairman. And we have covered a lot of ground here this morning. Thank you so much for coming and at least educating me on this process.

I just had a couple of general questions about the industry. Mr. Gorelick, you are in the business, and I just have a general question, what keeps you up at night?

Mr. GORELICK. Well, there is a lot, obviously, we are in business, the competitive concerns are something that we spend a lot of time thinking about, making sure that we are keeping up with changes in the market, and competitive changes and competitive dynamics, and that is where I spend a lot of my time thinking.

In terms of sort of risks to the market, I really worry about new regulation coming in, in ways that distorts how things are working pretty well right now.

Mr. ALLEN. Yes.

Mr. GORELICK. Things can always get better, and we should always be working to improve. I don't want to defend the *status quo*, however, some of the rules that are being proposed here and in other contexts definitely run the risk of unintended consequences that could make it a lot harder to manage risk, and that could take a lot of time and energy away from sort of our core functions of risk

management, and keeping up with competitive developments in the market.

Mr. ALLEN. Yes. I am on another committee, Education and the Workforce. We have had a number of hearings on the fiduciary rule. Does that in any way affect your business, or are you familiar with that?

Mr. GORELICK. I am not.

Mr. ALLEN. You are not, okay.

As far as your customer base, and again, this is just to satisfy my curiosity, your customer base, are they pretty much investors that know this industry, know this business, or are they folks that just kind of come and go in the market, and what incentives do people have to invest in these trades?

Mr. GORELICK. Sure. So we are a proprietary trading firm. So we manage—

Mr. ALLEN. Okay.

Mr. GORELICK. We trade our own capital. We put our own money at risk in all the trades that we conduct. So we don't have direct customers in the traditional sense.

Mr. ALLEN. I see. Okay. So from your standpoint then, as far as these regulations, if you are dealing with your own money what then would be the issues as far as the government is concerned?

Mr. GORELICK. Well, as proprietary traders, we clearly have incentives to make sure that we are managing our own risk. It is our own capital at risk, and so we are largely aligned with the goals of risk management throughout the market.

Mr. ALLEN. I see. Okay.

Mr. GORELICK. So I would think that that is the case.

The interest of the government here is sort of protecting market integrity, and we very much share that concern. We want to make sure that we are participating in markets that are transparent, that are well-regulated, and that the public rightfully has confidence in.

Mr. ALLEN. And that is one of the things that I have seen as far as my short time here, is that we have this tremendous disconnect between the regulatory part of this body *versus* actually the business community out there. And it sound like you all have put in a lot of your own regulatory environment to protect the industry, and I commend you on that.

As far as what we can do as a Committee, and I will leave this, I have about a minute and a half left, what is the biggest thing we can do here as this body to protect the integrity of this industry, and certainly as far as our role in agriculture?

Mr. GORELICK. The continued oversight responsibility of the Commission is very helpful. Holding hearings like this where you surface issues, and help to urge the Commission to continue to take into account the views of industry, and to identify where there are opportunities to improve the current regulatory framework.

Mr. ALLEN. Mr. Wood, do you have any comment?

Mr. WOOD. I would absolutely echo what Mr. Gorelick said there. From the FCM perspective, obviously, we have put a lot of investment into ensuring that we have the controls in place to obviously aid us in how we do our business in providing access to market participants, who are our customers. We would like to see a fair

and evenhanded continued regulation of the U.S. futures markets that is not too prescriptive or onerous or burdensome on the market participants.

Mr. ALLEN. Yes. And I assume you will holler at us if it gets a little too restrictive? Good.

Well, I am out of time. I will yield back.

The CHAIRMAN. The gentleman's time has expired.

Mr. BENISHEK, 5 minutes.

Mr. BENISHEK. Thank you, Mr. Chairman. Thanks, gentlemen.

I missed your initial testimony, but I have a couple of questions, I am not as sophisticated as far as this market stuff as some of these people here. What are some of the disruptions to the marketplace that, I think it was Mr. Vrabel described, like 20 or 30 incidents of market disruptions that have resulted from, I don't know, programmatic trading policies, or something? Can you explain that to me a little bit more, what happened, and like pick a couple of examples, and then how did you fix it or what happened there, tell me about that?

Mr. VRABEL. Sure. And just for clarity, the 15 to 30, or 15 to 20 disruptions in the market based on my understanding of that study, it was not disruptions that were the result of algorithmic trading malfunctions, which is important to recognize.

What we do though on a regular basis is monitor our markets for aberrations. And it could be as simple as we see a firm sending in a significant number of order messages over a given period of time, which may be indicative that their systems are malfunctioning. So this could have no impact on the marketplace at all, but we see conduct from that firm that seems like an aberration. And our ordinary course of practice is to reach out to that firm to try to identify the cause of that. And by and large, this causes the firm to say, "Yes, we realize the issue, we have implemented these new controls to prevent this from happening in the future." That is how we monitor the markets and mitigate the potential of an algorithmic trading disruption. And that is really what is important that, in order to protect the market, you have to spend a lot of time working with the participants, rather than imposing very—

Mr. BENISHEK. Does this happen very fast though? I mean it seems to me that these kind of algorithmic trading—that stuff happens really fast. I mean is there an opportunity to get in there and question them how this is working?

Mr. VRABEL. It is. CME Group has a number of controls that are in place. One of them is a messaging throttle control. And what it does is, it imposes a threshold where if a firm breaches that threshold over a given period of time, we start to reject new orders that that firm is submitting. And if it gets egregious enough, we actually shut down their access to the exchange. So we have controls that can act much faster than I can look at my computer screen and see what is happening.

Mr. BENISHEK. Right. Right. So how often does that happen?

Mr. VRABEL. I don't have numbers at-hand. I would say that it is not infrequent that firms have activity that causes us to prevent those orders. I would also say it is not always a malfunction.

Mr. BENISHEK. Right.

Mr. VRABEL. Sometimes it could be intended activity based on the market moving.

Mr. BENISHEK. Let me kind of go a different direction a little bit. Apparently, this Reg AT, if the participant violates an algorithmic trading policy, that is considered grounds for the CFTC to enforce, which seems kind of weird to me that your own rules, if you violate them. So what is to prevent you from writing very lax rules and then not reporting to the CFTC? I am just kind of curious about that.

Mr. GORELICK. That is one of the concerns that we have raised with the CFTC, that it sort of provides a disincentive for people to have particularly restrictive internal policies and procedures, and that the incentive that would come from that would be to have the bare minimum that are required by law to make sure that you are not inadvertently bringing on additional liability to your firm. So that is one of the definitional issues that we have suggested need to be fixed.

Mr. BENISHEK. All right. Thank you.

Thanks, Mr. Chairman. I will yield back.

The CHAIRMAN. The gentleman yields back.

Mr. LaMalfa, 5 minutes.

Mr. LAMALFA. Thank you again, Mr. Chairman. Please forgive me for having been in a different committee, if anything I ask may be a little redundant, having missed some of your previous testimony.

But, coming back to the requirement that firms make their source codes available without a subpoena at CFTC is very concerning to everybody here today. It would seem to me that this change is really an important issue of privacy and protection of intellectual property. So do any of you on the panel have any additional thoughts about how this agency could modify the code repository requirements in order to maintain that intellectual property? Anything you want to sum up with here?

Mr. GORELICK. So one of the things that I suggested in my written testimony is that there is an opportunity for a sort of principles-based retention policy for source code that, working with the industry, could be defined in a way that is consistent with current practices, to ensure that when the CFTC needs access and gets a subpoena, and follows proper due process, that they can be comfortable that the source code still exists within the firm in a reasonable way.

Mr. LAMALFA. With a subpoena.

Mr. GORELICK. With a subpoena, absolutely.

Mr. LAMALFA. Which isn't the pattern and doesn't seem to be the policy coming forward?

Mr. GORELICK. Correct. So this is a change that we are suggesting, an alternative that we are suggesting would be that a thoughtful principles-based retention policy should address the concern that the source code just doesn't exist, but in order to access that, the CFTC would have to follow existing practices of using a subpoena and following the due process, and putting in place appropriate safeguards.

Mr. LAMALFA. Gentlemen, do you wish to address that? Mr. Vrabel? Okay. All right, thank you.

The cost-benefit analysis, do you think there are really any benefits with the applications as to the end-users, the commercial end-users? Are they going to see anything they can put their finger on as a benefit? Gentlemen? Anybody? Don't want to touch that one?

Mr. GORELICK. Yes, I don't think it will be very measurable.

Mr. LAMALFA. Not very measurable, okay. Okay.

There is a questionable interpretation of a long-time definition of *floor trader* that is my understanding. Do you think it takes into account the costs of floor registration with this new definition, and ongoing cost of compliance?

Mr. GORELICK. I would say in general, if the rule were to be approved in its current form, or close to it, it would impose significant costs on both the industry participants and on the Commission in trying to enforce it and keep up with it, and those need to be factored into account. Ultimately, those costs are not just borne by the professionals in the market, they do get passed onto the end-users in the form of—

Mr. LAMALFA. Certainly. Everything does.

Mr. GORELICK.—higher transaction costs, less liquidity. I think that is something that we do need to be concerned about.

Mr. LAMALFA. So you don't think these costs are being taken into account by CFTC? This is being imposed. They are not really looking at that.

Mr. GORELICK. It did not seem to me from the cost-benefit analysis that they were looking at the broader impacts, that they were really looking at sort of more specific narrow cost concerns.

Mr. WOOD. I would echo that, yes, there is a wider concern that the cost-benefit analysis in the proposed rulemaking didn't take into account what the potential impact on the marketplace would be from the burden of compliance with Reg AT.

Mr. LAMALFA. It is kind of important to have that impact taken into account, isn't it? Yes, okay.

Thank you. I appreciate the panelists here today. Thank you, Mr. Chairman, for your graciousness.

The CHAIRMAN. The gentleman yields back.

Mr. Davis, 5 minutes.

Mr. DAVIS. Thank you, Mr. Chairman. I appreciate all the panelists.

Something like this seems that in this case we have market participants, and if you were given an opportunity to make comments, it seems like your comments weren't heard before the rule was implemented, otherwise we wouldn't be having this hearing today. So it is interesting, sitting on this side, to see that. And that is a concern to us.

And I do want to start a question with Mr. Vrabel. And I want to know what will the CME do with all of the data that AT persons and FCMs are required to report under Reg AT?

Mr. VRABEL. Under the requirements of Reg AT as it is currently drafted, not much. And here is the reason why. For example, the compliance reports that every AT person in a clearing firm would have to submit to the exchanges on an annual basis, the requirements in the draft would only require us to review those every 4 years. So we impose this burden on every firm to submit annual reports that the exchanges aren't obligated to review. So it leaves

huge gaps where participants are submitting these reports, thinking that the exchanges are endorsing them because they have submitted them, when, in fact, they may have risk controls that are inadequate.

Mr. DAVIS. Well, will this information help you reduce the risk of an algorithmic trading disruption?

Mr. VRABEL. From our perspective, no. As has been discussed earlier, the algorithmic trading disruptions and the malfunctions that are caused from algorithmic trading, in order to ascertain the root cause of those requires highly complicated analysis; the type of analysis that won't be gained from routine annual compliance reports that are submitted to the exchanges.

Mr. DAVIS. And I apologize if you may have addressed this in your opening testimony, but were these concerns raised during the comment period?

Mr. VRABEL. They were.

Mr. DAVIS. And the result?

Mr. VRABEL. There was no result.

Mr. DAVIS. Yet.

Mr. VRABEL. CME asked the Commission to extend the initial deadline so that we and others could come forward with more robust proposals, and that request was declined.

Mr. DAVIS. It was declined?

Mr. VRABEL. It was declined. We are thankful that the Commission reopened the comment period. Unfortunately, it was on a very small subset of the total proposed rule.

Mr. DAVIS. Well, I would hope that they would take comments into consideration more seriously that we are hearing from many of you as the market users.

Mr. Gorelick, or actually, the whole panel if you would like to answer this, do you believe that Reg AT's cost-benefit analysis fully appreciates the ramification of Reg AT on market participants in terms of initial and ongoing cost of the compliance? Whoever wants to start.

Mr. WOOD. Generally as a panel, we feel that the cost-benefit analysis focused on certain aspects, but not on wider aspects. In terms of compliance with what is proposed in the full scope of Regulation AT, it has a very large burden on pretty much all market participants, from those who would be classified as a floor trader, those who are already registered with the CFTC, perhaps as a commodity trading advisor or commodity pool operator, who would find themselves in the category of an AT person. It imposes a burden on the FCMs in terms of what we have to do providing access to an AT person, and the reporting responsibilities, and it poses a burden on the DCMs, in terms of what they have to do in providing additional controls, and the reports that have to be filed with everyone. That cost of compliance, unfortunately, will get passed on to the wider marketplace, so every type of market participant, whether they are commercial end-users, pension funds, asset managers, *et cetera*, in the that sense our main concern about Regulation AT is that this has a potentially large impact on how liquidity is provided in the U.S. futures markets that will ultimately be to the detriment of the end-user.

Mr. DAVIS. All right, thank you.

Mr. Gorelick, I don't have much time left so I want to ask you a specific question on this. Do you believe that the cost-benefit analysis fully appreciates the potential costs of an inadvertent release of your intellectual property?

Mr. GORELICK. No, that was not an area that was explored in the cost-benefit process, to my recollection.

Mr. DAVIS. Okay. And any other comment you would like to make on this follow up.

Mr. GORELICK. Sure. I would say one thing that often gets lost in these cost-benefit analyses is the competitive impacts of this regulation. When you have burdensome regulations like this, the result is the biggest firms can keep up with it, they can hire a few more compliance people, they can deal with the reporting requirements, they can handle it, but it is the smallest firms that sort of drop out of the market because they can't compete. And that has a negative impact in the competitiveness of the market in the short, medium, and long-terms.

Mr. DAVIS. Thank you very much.

My time has expired.

The CHAIRMAN. The gentleman's time has expired.

Mr. Neugebauer, 5 minutes.

Mr. NEUGEBAUER. Thank you, Mr. Chairman.

Mr. Gorelick, in your testimony, you stated that foreign governments such as China are seeking to impose similar source code requirements on U.S. firms. Could you describe some of those efforts?

Mr. GORELICK. Sure. I would actually refer the Committee to a comment letter that was put in by a variety of technology trade associations and industry associations that deals extensively with the source code issue. They raise a number of actions in which the Chinese Government sought to impose a source code requirement on U.S. companies who were selling technology into China in certain sectors, and ultimately, they were persuaded that this was unprecedented, not usual in the marketplace, and backed down from that requirement. The concern would be that this type of precedent that we would set would give excuses across the board in lots of different industries to impose similar requirements, which would be very detrimental to American IP protection globally.

Mr. NEUGEBAUER. Yes, with a country we already have a problem in that area, quite honestly.

Mr. Gorelick, Mr. Vrabel, or Mr. Wood, what risk controls would Reg AT impose on market participants that are not currently being implemented? Are there new risk controls that will be required in implementing this?

Mr. WOOD. With the way Regulation AT is currently proposed, it comes across as a very prescriptive list of risk controls that an AT person and an FCM and a DCM should have in place. And several of those controls are already in use on a wide basis, but several of those controls are not. And as a more general concern, it is too prescriptive in how those controls should be applied in various places. And the view of the industry is generally the controls that are used should be appropriate to the type of activity, and to the market participant in terms of how they manage their risk, how the FCM manages the risk of providing access to the customers, and how the DCM manages the risk to how it protects the market-

place, as opposed to being as prescriptive in the way Reg AT is currently proposed.

Mr. NEUGEBAUER. Yesterday, I chaired a committee a hearing on Fintech, and Fintech is a big world. And one of the things that keeps coming up is that people are coming up with innovative ways to make money and new business models, is that the regulatory community in many cases don't understand the technology, and in many cases maybe don't always understand the particular business model being imposed there. And so my concern is, and I wanted to hear your thoughts, my concern is, we see this innovation in the marketplace, and hopefully it makes markets more open, more efficient, and brings more liquidity to those markets. Do you sense that the regulatory community is kind of behind the curve and trying to play catchup, and trying to then fold some of this new technology and these methods into old regulatory framework?

Mr. GORELICK. I think that is a challenge in any regulatory environment, to keep up with technology, and I think that is something that we are seeing right here. And because there are new things going on in the market with new technologies that are constantly changing, we see the CFTC in one action try and catch up with every possible outcome of some of the changes that have occurred in the market in one rulemaking, and that is complicating the process a little bit. There is a consensus across the industry that the place to start is with risk controls, with pre-trade risk controls, and that there is an opportunity to really catch up a lot by focusing there, and then we can move elsewhere.

I would say another area where the regulators can sort of improve their capabilities is their data analytics ability. When there are lots of people out there who look at market events and say, "Wow, this looks strange," and they come up with their theories about what happened. The regulators are the expert agency who is well-placed to actually look at what occurred, and tell the public that this is what happened, and be reassuring where there is a need to be reassuring, and actually go and start enforcement or other compliance actions where there is a need to do that. Data analytics is another area that would help the Commission catch up very quickly.

Mr. WOOD. If I might just add there. We have seen the U.S. futures markets evolve in the space of 15 years from being 100 percent floor-driven, to screen-driven, to now, as we were talking earlier about the high prevalence of some form of automated trading. We believe that regulations should be principle-based to allow for continued evolution, especially in markets that are very technology-driven, and obviously where innovation is constantly occurring. And to that point, what is proposed in Reg AT is too prescriptive and anchors you in a period of time that doesn't necessarily allow for innovation and continued evolution.

Mr. NEUGEBAUER. I thank the Chairman.

The CHAIRMAN. Thank you. The gentleman's time has expired.

I want to thank our witnesses.

Let me follow up, Mr. Vrabel, you mentioned that the algorithmic trading users would, under your scheme, certify something, certify that they have tested. What were you asking to be certified, and who would set those standards, and would there be an outside, I

am a CPA by profession, and that word *certify* is a bit protected, but what would that look like, what would that certification look like?

Mr. VRABEL. Sure. A certification could look like a firm, an automated trading firm verifying that they are in compliance with a principle-based Reg AT regime. I can tell you that today, we require firms to submit those types of certifications on their maintenance of Audit Trailing, their 5 year retention requirements. And I can tell you with 100 percent certainty that if a firm does not believe it is in compliance, it will not certify that they complied with our rules. That causes us to then go interrogate the data and find out the reason why. And we have no reason to believe why that type of model that is currently enforced in FINRA, in a much more complicated securities world, wouldn't work in our environment.

The CHAIRMAN. All right.

Well, I want to again thank you. I am hard-pressed to envision a circumstance where the CFTC could have on-staff a cadre of people who would pick out one of these firms at random, and go in and drag through their source code in enough detail to find that glitch that had been missed, and looking to prevent some disruption in the market. If I had a client who was cooking the books, I didn't argue as to whether or not their automated general ledger system worked properly or not, I regulated what came out of it and go about that direction. So this whole issue around source code and those things, to me, seems to be wrong-headed, and I don't know that it gets us much.

On an after-the-fact, if someone has actually caused a disruption in the market, the violation is not going to be that they screwed up the code, the violation is going to be that they manipulated or hammered the market. And we don't really care how it happened if we can prove what they did. And it is a real head-scratcher for me to understand the agency's fixation on getting source code, having it in their own control, because I don't know what they would do with it. They get a lot of data today that I don't think they necessarily do everything that they should be doing with it, and this would just add more to that as well.

I did not hear from any of you that you don't want this arena regulated, that the conduct should just be free-flowing and *laissez-faire*, not one of you mentioned anything that remotely said this does not need to be regulated, but you did say that it ought to make sense and ought to be principles-based, as Mr. Wood just mentioned. And I am hopeful that this hearing and I see some representatives from the agency and others here, that the CFTC will respond to the comments made today, as well as the attention we have placed on this. But, the testing that I know Richard does on his team, as a market participant, if you had an algorithm you put in place and it did something you didn't want it to do, and it didn't disrupt the market but it caused you to be on the wrong side of all those trades, you have a vested interest, a proprietary interest, in not having a system that does something you don't want it to do. And that is that first layer, and then all the various things we could put in place on top of that that gets to the system. And this proposed rule has a lot of fine-tuning that needs to be done. I was particularly disappointed to hear that the cost-benefit analysis was

not maybe as fulsome as it should have been. Chairman Massad and I have a running argument as to the way the CFTC does their cost-benefit analysis. I don't believe CFTC takes into consideration the costs to market participants broadly, and I don't think it takes into consideration the costs to the agency itself. If I want to build a fiefdom then I could build all kinds of regulatory schemes, it causes me to have to beef-up my staff, to put in place that cadre of 50 or 60 different expert software engineers to put on my team so that I can wade into your software. Well, that makes no sense if, at the end of the day, it doesn't really prevent manipulation of the market.

The other thing that earlier on was said somehow that this regulatory scheme is going to be perfect, and that nobody will be able to violate it. Well, if that is the case, then perhaps the CFTC has discovered a technique that we could use perhaps in the real criminal area, and maybe write rules that nobody gets murdered today, and all those kind of good things. There is a lot of work to be done in this.

Again, thank you very much for you very clear testimony. It was great having you with us today.

Under the rules of the Committee, the record of today's hearing will remain open for 10 calendar days to receive additional material and supplementary written responses from the witnesses to any question posed by a Member.

This hearing of the Committee on Agriculture is adjourned. Thank you.

[Whereupon, at 11:54 a.m., the Committee was adjourned.]

[Material submitted for inclusion in the record follows:]

SUBMITTED STATEMENT BY SUSAN BERGLES, ASSISTANT GENERAL COUNSEL,
AMERICAN GAS ASSOCIATION

The American Gas Association (“AGA”)¹ appreciates the opportunity to submit this statement for the record relating to the Commodity Future Trading Commission’s (“CFTC”) proposed rule on Regulation Automated Trading (“Regulation AT”).² AGA filed comments to the CFTC in this proceeding on March 16, 2016.

The potential impact of proposed Regulation AT on AGA’s members is not insignificant. Absent an appropriately tailored and modified definition of “Algorithmic Trading,” AGA believes there would be a strong disincentive for AGA members and other commercial end-users to use Direct Electronic Access (“DEA”) for futures trading activity on or subject to the rules of a Designated Contract Market (“DCM”). AGA’s comments also expressed concern about the requirement that, for the first time, commercial end-users might be deemed “floor traders” and have to register with the CFTC based solely on the manner in which they trade—and the potential for Regulation AT, if applicable, to unwind or render inapplicable many of the provisions in other rules put in place to limit the burden and costs for commercial end-users, such as AGA members.

As users of the futures markets, AGA members support and appreciate the CFTC’s efforts to bolster safeguards and risk controls in order to protect against the risk of malfunctioning algorithmic trading systems, and to increase transparency. However, AGA submits that it is vitally important that any new rules promulgated as part of Regulation AT preserve, and do not negatively impact, the ability of commercial end-users to access the futures markets and use futures as part of their risk management tools. Specifically, AGA is concerned that proposed Regulation AT sweeps too broadly in its reach, and as such, may: (1) have the unintended consequence of hindering the ability of commercial end-users to efficiently and cost-effectively access the futures markets; and (2) create inconsistency and regulatory uncertainty regarding issues that commercial end-users and the CFTC just recently addressed in other rules, such as margin requirements for uncleared swaps (the “Margin Rules”), and record-keeping requirements.³ AGA believes that the CFTC need not, and should not, deem end-users to be floor traders *solely* because they utilize DEA for “Algorithmic Trading.”

Simply put, AGA’s concern regards the impact of proposed Regulation AT on its commercial end-user members that may transact in futures contracts via DEA to a DCM for “Algorithmic Trading.” As proposed, the definitions, including “Algorithmic Trading,” “DEA,” and “floor trader,” are so broad and far reaching in scope that they may have the unintended consequence of actually discouraging companies looking to hedge their commercial risks from trading futures. In particular, commercial end-users could—with just one DEA futures transaction—fall within the definition of a “floor trader” which requires registration with the CFTC, and concurrently fall within the definition of an “AT Person” subject to all the requirements of Regulation AT.

Additionally, AGA is concerned that proposed Regulation AT potentially would impact the commercial end-user’s status under other rules that the CFTC has recently adopted or amended that address concerns raised by end-users. Becoming a “floor trader” by virtue of Regulation AT may inadvertently result in commercial end-users becoming “registered members” for purposes of the CFTC’s general record-keeping rules, specifically Rule 1.35(a). AGA submits that this would be an unfortunate step in the wrong direction, given this rule was recently amended to provide that commercial end-users as “Unregistered Members” do not have to retain pre-swap-trade communications or text messages or link all relevant data to a particular swap. Additionally, AGA is concerned that because “floor traders” fall within the defined term “financial end-users” for purposes of the CFTC’s recently-adopted

¹The AGA, founded in 1918, represents more than 200 local energy companies that deliver clean natural gas throughout the United States. There are more than 72 million residential, commercial and industrial natural gas customers in the U.S., of which 95 percent—just under 69 million customers—receive their gas from AGA members. For more information, please visit www.aga.org. AGA member companies provide natural gas service to consumers and businesses under rates, terms and conditions that are regulated at the local level by a state commission or other regulatory authority with jurisdiction. They use financial tools to hedge the commercial risks arising from the regulatory obligation to provide affordable, reliable natural gas service to customers—risks that include commodity price volatility. These tools may include futures contracts traded on CFTC-regulated exchanges, and over-the-counter energy derivatives.

²*Regulation Automated Trading*, 80 FED. REG. 78824 (Dec. 17, 2015) (“Proposed Rule”).

³See *Margin Requirements for Uncleared Swaps for Swap Dealers and Major Swap Participants, Final Rule and Interim Final Rule*, 81 FED. REG. 636 (January 6, 2016), and *Records of Commodity Interest and Related Cash or Forward Transactions, Final Rule*, 80 FED. REG. 80247 (December 24, 2015).

Margin Rules, commercial end-users that are “floor traders,” solely because of their automated trading in futures, would be subject to margin requirements in their swap trading. Thus, the potential impact on commercial end-users of the definitions in proposed Regulation AT would not be insignificant.

Further, the proposed definition of DEA appears so broad as to include tools that DCMs are marketing, and make available for use by commercial end-users, including AGA members. The definition of DEA could be interpreted to include these common order management tools even if they include DCM-administered risk controls and, notably, even if the market participant is accessing the DCM via a Futures Commission Merchant (“FCM”) with additional risk controls. As such, end-users may not be able to use these DCM-administered tools going forward—notwithstanding that the use of these tools may result in decreased fees—due to the high cost and burden that would be associated with the Regulation AT rules. AGA submits this result is not in line with the CFTC’s commitment to minimizing the burdens and costs of its regulations on commercial end-users.

AGA believes that subjecting all commercial end-users that use DEA to access the futures markets to the comprehensive and substantial requirements in proposed Regulation AT—including the requirement to register with the CFTC—would run counter to the CFTC’s laudable recent efforts to fine-tune its regulations to make sure that commercial businesses can continue to use the futures markets effectively. AGA appreciates that it has been a priority of the CFTC to make sure the overall regulatory scheme it puts in place recognizes the needs and concerns of commercial end-users, and that the overall framework is designed to minimize burdens on commercial end-users who depend on the markets to hedge normal business risks.⁴

The American Gas Association appreciates the House Agriculture Committee’s careful review of the CFTC’s proposed Regulation AT. The impact of this rule on end-users, notably gas utilities, may indeed be substantial, burdensome and costly. We look forward to working with the Committee, the CFTC and all other impacted parties to see that this matter is settled appropriately.

Respectfully Submitted,



SUSAN BERGLES,
Assistant General Counsel,
American Gas Association.

○

⁴*Opening Statement*, Chairman Timothy G. Massad, Open Meeting on Proposed Rule on Margin Requirements for Uncleared Swaps and Final Rule on Utility Special Entities (September 17, 2014).