TWO SIGMA

Two Sigma Investments, LP
100 Avenue of the Americas, Floor 16
New York, NY 10013

T +1 212 625 5700
F +1 212 625 5800
www.twosigma.com

By Electronic Submission

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

Re: **Notice of Proposed Rulemaking on Regulation Automated Trading, RIN 3038-AD52**

Dear Mr. Kirkpatrick:

Thank you for the opportunity to comment on the proposed Regulation Automated Trading ("Reg AT"). Two Sigma[1] applies a process-driven, algorithmic approach to investment management. We perform quantitative analysis to build mathematical strategies and implement those strategies using technology-driven investment, optimization, risk management, and execution techniques. These strategies and techniques guide our investment decisions in financial instruments regulated by the Commodity Futures Trading Commission ("Commission"). As our two investment managers are both registered as a Commodity Pool Operator ("CPO") and as a Commodity Trading Advisor ("CTA"), we would be affected by a number of provisions in Reg AT if it were adopted as proposed.

The Commission has undoubtedly received large volumes of comments addressing technical aspects of Reg AT and its impact on the market. We are active members of various trade associations and strongly support the letters they have submitted on behalf of their memberships. However, we write separately to focus on an issue that is of the utmost importance to Two Sigma – fostering innovation. To us, innovation means thoughtfully pursuing technology-driven, creative ideas and solutions that seek to generate improved returns for our clients and that aim to continuously improve upon existing methods. Innovation is linked inseparably with the safeguarding of intellectual property.

Technology is at the heart of what we do at Two Sigma. We harness technology to better understand the markets and to best serve our investors. Principles-based regulation has

[1] Two Sigma is a family of financial services companies, including two investment managers (Two Sigma Investments, LP and Two Sigma Advisers, LP) and a FINRA-registered broker-dealer (Two Sigma Securities, LLC).

allowed us to develop our technology in a way that we feel is well controlled and benefits our clients. While we applaud the Commission for its efforts to ensure that regulation keeps pace with the advent of new technologies and that the markets remain safe and fair, we would encourage you to reconsider some provisions in Reg AT that could diminish intellectual property protections, prescribe technological choices by firms, or even worse aid cyber criminals in order to ensure that innovation continues to be fostered and encouraged, not stifled or deterred.

As proposed, Reg AT requires registrants to make large volumes of their most sensitive data available without corresponding policies and procedures to protect their intellectual property. The Commission's goals can be advanced through more effective, less risky measures.

As proposed, Reg AT raises concerns about the adequacy of the Commission's protections for sensitive data obtained from registrants. Reg AT will result in the Commission accessing and housing significantly more data from its registrants than it does now. As this data could contain the trade secrets of hundreds of registrants, the Commission will become a ripe target for hacking and cyberattacks. In the absence of strong confidentiality protections and protocols to prevent such incidents, we have genuine concerns about exposing our sensitive intellectual property. And while the confidentiality protections we would encourage you to apply to sensitive data may be sufficient for the vast majority of information at issue, we have serious concerns over disclosing our most sensitive intellectual property without due process regardless of the confidentiality policies and procedures in place.

Source code should be preserved, but not treated as books and records or housed by the Commission.

Why is this concern so important to us? The source code of our investment and execution algorithms and models, along with related descriptions of the code, such as white papers, are the core intellectual property of firms like ours. These are our trade secrets – literally, the hard-won, analytical insights by which we make investment and trading decisions. We are able to dedicate both ourselves and significant financial resources to creating innovative strategies to better serve our clients because we are confident in the cybersecurity protocols and employee safeguards we have implemented to protect our work.

The protections we have put in place are essential because of the nature of our innovations. While our trade secrets take tremendous resources and effort to create, in their final form they are often relatively scalable and portable. This information, even at

the highest level of generality, provides a roadmap to make profits in the market and would provide someone an unfair shortcut to the ideas our clients pay us to develop. The disclosure of this information would, over time, undermine or destroy a firm's ability to continue using the disclosed strategies. As highly regulated entities, CPOs and CTAs subject their trade secrets to many layers of risk controls and regulatory checks throughout the process. However, if an ill-intentioned individual committed to disrupting and harming the market was to obtain, via cyberattack or otherwise, the trade secrets of regulated firms collected under Reg AT along with the vast amount of market data also held by the Commission, the consequences for the market could be dire and have serious impacts across the entire global economy. Such a disclosure would empower bad actors to use the information in an unregulated, malicious way that inflicts real damage to the markets regulated by the Commission and the global economy. In short, the disclosure of trade secrets would severely compromise a firm's ability to function and could ultimately harm its investors and the market.

It is worth underscoring the fact that the confidential strategies we use on behalf of our clients cease to work when they become common knowledge or are overused. If a firm's strategies were revealed to the market, other traders could copy those strategies or even trade against them; they would cease to be effective and require a firm to develop new strategies in order to generate returns for clients. In all likelihood, that firm's clients would move their money to other firms not facing an extensive rebuilding process, and the victimized firm would go out of business.

With the consequences of the disclosure of this information so great for both individual firms and the market generally, we are deeply concerned at the prospect of this sensitive information leaving our highly secure systems or entering the minds of those beyond our trusted employees. There is no greater risk we face to our business than the disclosure of our trade secrets. A key element of the growth of research and technology in the United States has been the confidence that innovations will be protected by U.S. law and kept safe from misappropriation. The nature of our innovations means their public disclosure would erode their efficacy and cripple our business. As a result, we do not patent or copyright our algorithms or proprietary software. Instead, our only legal option to protect our innovations is as a trade secret. Trade secret protection depends on our efforts to prevent unauthorized disclosure of our confidential information and, as proposed, Reg AT inadvertently lessens those protections. That threatens not only firms like ours, but the market at large since the innovations behind algorithmic trading have been broadly adopted to improve market efficiency and reduce transaction costs for investors and end-users alike.

Despite our concerns with the collection and housing of our most sensitive information outside of our systems, we agree with the Commission that registrants should be required to preserve their source code. Preserving key source code within a firm is the industry's best practice and is the approach we follow at Two Sigma. However, treating the source code of algorithmic traders as a book and record under 17 CFR 1.31 is inconsistent with the sensitivity of the information in question. As Commissioner Giancarlo's November 24 statement on Reg AT noted, treating source code as books and records "dramatically lowers the bar for the federal government to obtain this information."

Our concerns would be magnified if the Commission were to propose a third-party escrow or examination of our sensitive information. We do not utilize these services, and neither do our peers, because we do not believe they provide sufficient protection for our trade secrets. While a source code retention requirement is consistent with the approach our industry uses to maintain the confidentiality of its trade secrets, requiring third-party escrow of our trade secrets presents the same concerns as the Commission housing our trade secrets, but in a heightened way due to the concern of turning over trade secrets to a non-governmental entity with which we do not share the same relationship of trust.

Thankfully, a clear alternative approach exists that will ensure the Commission has access to the information it needs while also mitigating our concerns regarding the disclosure of our trade secrets. We strongly encourage the Commission to adopt the approach Chairman Massad has suggested in recent Congressional testimony where firms would be required to maintain source code, but not have to provide it to the government without due process and strong confidentiality protections.

In testimony before the House Agriculture Committee on February 10, 2016, Chairman Massad stated that the Commission is not seeking to house the intellectual property of registrants, but instead the Commission simply is asking registrants to preserve the information "so that if there is a problem and we do need to go get [the information] using the proper procedures, we can." The Chairman further testified that the Commission is "not asking [registrants] to turn [source code] over to us routinely. We're not asking [registrants] to file it with us."

As the Chairman noted, source code is already available to government regulators via an established process; either a request for voluntary production or compulsory production pursuant to a subpoena. Where voluntary production may not adequately address a registrant's concerns regarding the scope of the information sought or the confidentiality it will be afforded, the subpoena process ensures that the registrant receives adequate due process. The subpoena process can also be used to ensure that extremely sensitive information is handled with the necessary protections and better assuages the concern that

a registrant's trade secrets would be handled like routine data. We urge the Commission to move forward by working within the subpoena process if and when it needs to review a firm's most sensitive information.

Our concerns apply with equal force to both investment decision and execution strategies.

We would note that the concerns we have expressed regarding the protection of our strategies apply equally to both investment decision-making and execution algorithms. While some firms decide to focus their resources solely on investment strategies and rely on third-party or manual execution pathways, other firms in our industry have made execution research an essential element of their business.

At Two Sigma we strive to continually improve how we turn our ideas into action. To achieve that goal, we take the same innovative, technology-driven approach to execution as we do in the investment decision-making process. Our innovations in execution systems have enabled us to generate better returns and lower transaction costs for our clients than had we relied solely on third-party execution systems. If regulations governing execution systems are put in place as a result of Reg AT, a principles-based approach would allow us to continue innovating in a way that benefits our clients and the market while ensuring we comply with a comprehensive framework of regulation. But if the Commission were to seek to regulate automated trading via prescriptive rules or by housing all of a firm's execution strategies, the ability of a firm to safely and confidently innovate using methods that best suit that firm would be severely weakened.

Firms like ours have dedicated significant time and resources to continually improving execution strategies and capabilities. We are concerned that if these strategies were to receive less assurance of protection than other sensitive information provided to the Commission, many firms would choose to stop allocating their limited resources to enhancing execution or forego certain changes that could have ultimately benefitted the market and clients. We urge the Commission not to create a double standard where choosing to dedicate resources to innovating in execution leads to fewer protections.

The Commission needs stronger confidentiality policies and procedures in place to protect all sensitive information it gathers from registrants.

Even if the source code repository is modified as suggested above, the Commission should consider notably enhancing its confidentiality procedures and protocols to protect the information it gathers from registrants.

In his final weeks as a Commissioner of the Securities and Exchange Commission ("SEC"), Luis Aguilar outlined the immense value of the data that financial regulators collect from their registrants. He explained that when a regulator invokes "its authority to collect and analyze this information, [it] simultaneously acquires a countervailing obligation to protect it from misuse." But in their current state, the Commission's policies and procedures do not adequately protect the sensitive information received from registrants.

Under 7 U.S.C § 12, the Commission would be able to authorize the disclosure of the confidential information it receives under Reg AT with few limitations. The current state of these policies causes registrants to assume any information provided to the Commission can ultimately be released to the press, interested parties, or even the general public. While we trust the Commission's discretion and do not expect the Commission would approve such disclosures, the lack of formal prohibitions is deeply disconcerting to us.

Algorithmic investment management firms have spent billions of dollars over many years to develop sufficient safeguards to protect the sensitive information they possess. Our regulators and clients demand we have the most cutting-edge systems in place to ensure all of our data (and theirs) remains safe. We would ask the Commission put in place corresponding protections for the information it houses from its registrants and treat information gathered under Reg AT with at least the same degree of confidentiality that the information gathered during investigations currently receives. Until such protections are in place, we would request the Commission work with registrants to ensure sensitive information, where it can be of utility, is reviewed in a secure manner.

Another significant issue for confidentiality purposes is who will have access to the sensitive information collected as a result of Reg AT. The breadth of information available to those within the Commission who review information submitted in response to Reg AT far exceeds the access granted to all but the most senior employees of registrants. While code and underlying research is reviewed by the appropriate personnel before it is implemented, our control and compliance teams do not typically access this sensitive information to ensure that strategies and techniques are appropriately risk controlled and comply with applicable regulation. Instead, we have adopted a control framework that more closely resembles the development standards and risk controls required by other provisions proposed in Reg AT. Despite the integrity of Commission staff, the individuals who review the data of registrants can and do leave the government for opportunities with financial services firms. These individuals cannot forget the analytical insights they learned. As former Commission General Counsel Dan Berkovitz noted when the Reg AT proposal was released, "a person doesn't necessarily need the

original code to develop a trading strategy if he or she understands the contours of how other algorithmic traders operate." While we have the utmost respect for Commission staff, a codification of the relationship of trust we share would significantly increase our comfort with the Reg AT proposal.

Given the myriad ways that registrant-provided information can legally find its way out of the Commission and into the hands of the press and competitors, we encourage the Commission to put in to place robust confidentiality protections that go significantly beyond the existing framework.

The Commission should also take steps to ensure registrants and the public that its systems protect against cyberespionage.

In addition to concerns regarding the Commission's policies and procedures on confidentiality, the struggles the federal government has had with cybersecurity give us pause. The General Accounting Office found that federal agencies had 67,168 cybersecurity incidents in 2014 alone, and an Assistant Director of the FBI has told Congress that every federal agency has been a victim of cyberespionage.

The continuing threat of cyberespionage is particularly concerning for those who report to financial regulators, as cyber criminals around the world are well aware that the computer systems of financial regulators are currently an easy access point to the inner workings of the world's financial markets and investment firms. And as discussed above, the consequences of such a cyberattack would have serious consequences for both registrants and the market globally.

The information the Commission likely will receive because of Reg AT is invaluable. As Commissioner Giancarlo stated when Reg AT was proposed, "[a]ny data breach of this information would be devastating for such entities and, potentially, for the safety and orderly operation of U.S. markets." If the Commission intends to house this information, the Commission's cybersecurity protocols and systems must be among the nation's strongest. And just as importantly, registrants and cyber criminals need to know that those protocols and systems are strong. Accordingly, we would encourage the Commission to adopt and publicize enhanced cybersecurity protocols.

The combination of these concerns creates an uncertain environment that discourages innovation, or even participation, in the market.

Under the approach proposed in Reg AT, intellectual property protections could be diminished, cyber criminals could be aided, and prescriptiveness could alter the pace and

scope of technological innovations at regulated firms. It would also be quite difficult for a registrant to assert that the Commission, the Department of Justice, or an exchange had overstepped its bounds in taking possession of a firm's sensitive information, without any need for justification. As a result, algorithmic investment management firms would fear that their hard-earned insights could be taken or altered at any time and for any reason. With time, firms may divert their energy and resources to participating in markets that are not regulated by the Commission or investors may decide to reallocate their capital to managers not subject to Reg AT.

Because of this concern, Reg AT has the potential to fundamentally change the incentive structure that has led firms to innovate. The development of innovative strategies and techniques has allowed investors to have access to potentially higher returns than those available through products that simply track the market. But those innovations do not come freely. Firms and individuals will only innovate to the extent the regulatory framework allows them to do so without fear that their work will be compromised. By enhancing its confidentiality procedures and protocols, the Commission can ensure that the markets it regulates continue to attract innovation and the investment that follows it.

Respectfully submitted,

Matthew B. Siano
Managing Director, General Counsel