MANAGED FUNDS ASSOCIATION
The Voice of the Global Alternative Investment Industry
WASHINGTON, DC | NEW YORK

November 17, 2017

Via Electronic Submission

Mr. Thomas W. Sexton, III
President and Chief Executive Officer
National Futures Association
300 S. Riverside Plaza, #1800
Chicago, IL 60606-6615

Re: Protection of Confidential Registrant Information

Dear Mr. Sexton:

Managed Funds Association[1] ("**MFA**") has been concerned with data security and the protection or confidential registrant information by regulators. The recent cyber breaches of Equifax and the Securities and Exchange Commission were highly alarming and demonstrate the real risks and harm that can befall individuals and registrants when bad actors hack companies and regulators. As the National Futures Association ("**NFA**") oversees commodity pool operators ("**CPOs**") and commodity trading advisors ("**CTAs**") alongside the Commodity Futures Trading Commission ("**CFTC**"), MFA submits to NFA and the CFTC recommendations on the protection of confidential registrant information. MFA has four suggestions (outlined below) to ensure the efficacy of the CFTC's and NFA's regulatory programs while reducing the risks of inadvertent disclosures from cyber intrusions.

In recent years, the potential consequences of a cyber intrusion have grown considerably as the CFTC and NFA have obtained significantly more sensitive information from registrants, including from systemic risk reports, while the CFTC's information security vulnerabilities remain amongst its most serious management challenges.[2] MFA has raised strong concerns to regulators, including the

[1] The Managed Funds Association (MFA) represents the global alternative investment industry and its investors by advocating for sound industry practices and public policies that foster efficient, transparent, and fair capital markets. MFA, based in Washington, DC, is an advocacy, education, and communications organization established to enable hedge fund and managed futures firms in the alternative investment industry to participate in public policy discourse, share best practices and learn from peers, and communicate the industry's contributions to the global economy. MFA members help pension plans, university endowments, charitable organizations, qualified individuals and other institutional investors to diversify their investments, manage risk, and generate attractive returns. MFA has cultivated a global membership and actively engages with regulators and policy makers in Asia, Europe, North and South America, and many other regions where MFA members are market participants.

[2] *See, e.g.*, CFTC Office of Inspector General ("**OIG**") Assessment of the Most Serious Management Challenges Facing the CFTC, September 25, 2017, available at: http://www.cftc.gov/idc/groups/public/@aboutcftc/documents/file/oigmgmtchall2017.pdf; CFTC OIG Assessment of the Most Serious Management Challenges Facing the CFTC, October 26, 2016, (finding that the most serious management challenges for the CFTC are to minimize information security vulnerabilities in its network, and to execute its strategic plan with limited budgetary resources, among others) available at: http://www.cftc.gov/About/OfficeoftheInspectorGeneral/ssLINK/oigmgmtchall2015; CFTC Office of Inspector General ("OIG") Report to Congress, April 1, 2015-September 30, 2015, (raising concerns with the vast majority of

CFTC, regarding data security and the protection of confidential registrant information.[3] We are concerned that a data security breach could create significant market volatility, destabilize markets, harm investors, and result in the misappropriation of confidential proprietary information.

With the benefit of more experience, it would be wise for the CFTC and NFA to reconsider the types of information they collect and under what circumstances. We urge NFA to rethink: (1) the data it collects from CPOs and CTAs; (2) how it collects and protects such data; and (3) the disposal of such data when it is through using it.

I. Reviewing What the CFTC and NFA Collect

The CFTC and NFA require CPOs and CTAs to provide lengthy, detailed reports of their investments, strategies and business operations through Forms CPO-PQR and CTA-PR.[4] Additionally, NFA collects significant amounts of sensitive information from CPOs and CTAs in the course of routine examinations. In the current environment of growing cybersecurity threats, the "more is better" approach to data collection is no longer a pragmatic or prudent approach to regulation. As part of the CFTC's and NFA's strategies to mitigate systemic risk and harm to investors and registrants from cyber theft, we believe the CFTC and NFA should use greater restraint in their data reporting requirements and seek only data that they need to achieve their core missions.

Recommendation #1: The Commission and NFA should narrow the scope of systemic risk filings to information that could identify such risks to data that is necessary to achieve their core mission. To assist regulators in considering this request, MFA will be developing a revised Form PF/PQR, consistent with our recommendations for the CFTC and the Securities and Exchange Commission to rationalize and simplify reporting by adopting a single, simpler form; and for NFA to amend Form PQR to its pre-Dodd-Frank Act version and to make similar amendments to Form PR.[5]

II. Data Collection & Protection of CPO and CTA Filings

MFA supports the CFTC and NFA having the information they need to oversee registrants and to surveil markets. This authority, however, needs to be balanced with the potential risk of irrevocable harm (*e.g.*, unauthorized disclosure or misappropriation of trade secrets) to registrants and their investors. We believe the CFTC and NFA should each review how they collect and protect information through routine confidential filings and during regular exams to mitigate the damage from a future cyber breach.

---

servers and network users) available at: http://www.cftc.gov/idc/groups/public/@aboutcftc/documents/file/oig_reporttocongress093015.pdf.

[3] *See* letter from Stuart J. Kaswell, Executive Vice President, Managing Director and General Counsel, MFA, to Chris Giancarlo, Chairman, CFTC, dated June 6, 2017 on Regulatory Priorities, available at: https://www.managedfunds.org/wp-content/uploads/2017/06/MFA-Letter-to-Acting-Chair-Giancarlo-Appendix.pdf.

[4] Forms CPO-PQR and CTA-PR, available at: https://www.nfa.futures.org/EasyFilePlus/EFPTemplate.aspx?template=PQR; and https://www.reginfo.gov/public/do/DownloadDocument?objectID=28356201.

[5] *See supra* n. 3.

Recommendation #2: MFA believes the CFTC and NFA should incorporate protections within the design of their forms and reporting systems to mitigate cyber breaches. The CFTC and NFA should focus on disaggregating the information stored. For example, the CFTC and NFA should enable CPOs and CTAs to use alphanumeric identifiers for filings, to be kept separately within their systems, and revise questions containing firm identifying information. These safeguards would mitigate damage from a breach of EasyFile (through which registrants file Forms CPO-PQR and CTA-PR and other filings). It would be the equivalent of using a unique numerical identifier on a credit file, rather than the person's name and social security number.

Recommendation #3: The CFTC and NFA should have information security policies in which the protections and security requirements are heightened or tiered depending upon the level of sensitivity of the data collected. CFTC or NFA staff should have access to this sensitive information on a "need to know" basis and in accordance with pre-determined protocols.

III. Disposal or Return of Confidential Data

To further mitigate the risks from a future cyber breach, when the CFTC or NFA is through using registrant data—whether it be old Forms CPO-PQR or CTA-PR data or documents received as part of an exam request—we believe it is important for the CFTC and NFA to return or destroy such data, rather than maintain it in its network and prolong the risk of the data disclosure or misappropriation. Certain types of registrant information, such as trade secrets, may never lose their status as confidential proprietary information. Keeping years of old data or confidential information provides an attractive target for thieves, cyber or otherwise.

Recommendation #4: To further mitigate the risks from a future cyber breach, the CFTC and NFA should return or destroy sensitive, confidential registrant data once they are through using it.

* * * * *

MFA respectfully urges you to incorporate the above policy recommendations as you review NFA's policies and procedures for enhancing data security and how best to protect investors and markets. We would be happy to discuss these concerns with you or your staff in greater detail. If you have any questions or comments, or if we can provide further information, please do not hesitate to contact Jennifer Han, Associate General Counsel, or the undersigned at (202) 730-2600.

Respectfully submitted,

/s/ Stuart J. Kaswell

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

CC: Carol Wooding, General Counsel