



October 17, 2017

Via Electronic Submission: chairmanoffice@sec.gov

The Hon. Walter J. Clayton
Chairman
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: Protection of Confidential Registrant Information

Dear Chairman Clayton:

Managed Funds Association¹ (“MFA”) appreciates your leadership in addressing the recent cyber intrusion into the EDGAR system and the cybersecurity risks faced by the Securities and Exchange Commission (“SEC” or “Commission”). MFA has four suggestions, outlined below that could ensure the efficacy of the SEC’s regulatory program while reducing the risks of inadvertent disclosures from cyber intrusions.

As you have identified, the range of cyberattack perpetrators is broad, and the potential consequences of a cyber intrusion risks can be significant to market participants and the market overall.² In recent years, the potential consequences of a cyber intrusion have grown considerably as the Commission has obtained significantly more sensitive information from registrants via routine filings and examinations. The Commission’s view had seemed to be that collecting more information was always better, because the Commission and other agencies wanted to survey the landscape. The Commission sought such a broad collection of data despite the risks of such activity, and as a result the Commission has become a repository of confidential market moving information and proprietary intellectual property. In light of these developments, MFA has raised strong concerns to regulators, including the Commission, regarding data security and the protection of confidential registrant information. 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.

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 Statement on Cybersecurity, SEC Chairman Jay Clayton, September 20, 2017, available at: <https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20>.

We now believe that with the benefit of more experience, it would be wise for the Commission to reconsider the types of information that it collects and under what circumstances. You have recently stated that “even the most diligent cybersecurity efforts will not address all cyber risks”³ and because of this concern we urge the Commission to rethink: (1) the data it collects from advisers; (2) how it collects and protects such data; and (3) the disposal of such data when the Commission is through using it.

I. Reviewing What the SEC Collects

The SEC requires investment advisers of private funds to provide lengthy, detailed reports of their positions, strategies and business operations through Form PF.⁴ In addition, the SEC exam staff, including from the Quantitative Analytics Unit, requests large amounts of confidential, commercially-valuable intellectual property with respect to specific fund trading strategies. MFA supports providing systemic risk information to the SEC and an effective SEC examination program for investment advisers. Nonetheless, MFA is concerned with the Commission’s ability to protect the data it requests from registered investment advisers. 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 Commission’s strategy to mitigate systemic risk and harm to investors and registrants from cyber theft, we believe the SEC should use greater restraint in its data requests and request only data that it needs to achieve its core mission.

Recommendation #1: The Commission should narrow the scope of systemic risk filings to information that could identify such risks and of exam requests to data that is necessary to achieve the SEC’s core mission. To assist the Commission in considering this request, MFA will be developing a revised Form PF/PQR, consistent with our recommendations for the Commission and the Commodity Futures Trading Commission to rationalize and simplify reporting.⁵

II. Data Collection & Protection of Adviser Filings and Exam Materials

MFA supports the Commission having the information it needs 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 Commission should review how it collects and protects information through routine confidential filings and during regular exams to mitigate the damage from a future cyber breach.

Recommendation #2: MFA believes the Commission should incorporate protections within the design of its forms and reporting systems to mitigate cyber breaches. The Commission should enable

³ *Id.*

⁴ SEC Form PF, available at: <https://www.sec.gov/files/formpf.pdf>.

⁵ See letter from Stuart J. Kaswell, Executive Vice President, Managing Director and General Counsel, MFA, to Jay Clayton, Chairman, SEC, dated May 18, 2017 on Regulatory Priorities, available at: <https://www.managedfunds.org/wp-content/uploads/2017/05/MFA-Regulatory-Priorities-Letter-to-SEC-Chairman-Clayton.pdf>.

investment advisers to use an alphanumeric identifier for filings, to be kept separately within the SEC systems, and limit questions for firm identifying information. These safeguards would mitigate damage from a breach of the Investment Adviser Registration Depository (through which Form PF and other filings are made). 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: With respect to exams, we believe SEC exam staff should exhaust other less sensitive means of understanding a firm's activities before requesting for any confidential, commercially-valuable intellectual property. The SEC exam staff should only ask for such information if absolutely necessary and through the subpoena process. Further, we think the Commission should have an information security policy in which the protections and security requirements are heightened or tiered depending upon the level of sensitivity of the data collected, regardless of how it is collected (e.g., through Form PF versus through an exam).

III. Disposal or Return of Confidential Data

To further mitigate the risks from a future cyber breach, when the SEC is through using registrant data—whether it is old Form PF data or documents received as part of an exam request—we believe it is important for the SEC to affirmatively return or destroy such data, rather than maintain it in its network and prolong the risk of the data disclosure or misappropriation. Keeping years of old data or confidential information only provides an attractive target for thieves, cyber or otherwise.

Recommendation #4: To further mitigate the risks from a future cyber breach, the SEC should return or destroy sensitive, confidential registrant data once the SEC is through using it. Certain types of registrant information, such as trade secrets, may never lose their status as confidential proprietary information.

* * * * *

MFA respectfully urges you to incorporate the above policy recommendations as you review the Commission's policies and procedures for enhancing data security at the Commission and how best to protect investors and markets. 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: The Hon. Michael S. Piwowar
The Hon. Kara M. Stein
Lucas Moskowitz, Chief of Staff
Dalia Blass, Director, Division of Investment Management
Peter Driscoll, Acting Director, Office of Compliance Inspections and Examinations