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

March 15, 2019

The Hon. Mike Crapo
Chairman
U.S. Senate Committee on
Banking, Housing, and Urban Affairs
534 Dirksen Senate Office Building
Washington, DC 20510

The Hon. Sherrod Brown
Ranking Member
U.S. Senate Committee on
Banking, Housing, and Urban Affairs
534 Dirksen Senate Office Building
Washington, DC 20510

Re: Data Privacy, Protection and Collection

Dear Chairman Crapo and Ranking Member Brown:

Managed Funds Association[1] ("**MFA**") greatly appreciates the opportunity to share its views on data privacy, protection and collection. We agree and support your views that the "collection, use and protection of personally identifiable information and other sensitive information by financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) is something that deserves close scrutiny."[2] For several years now, MFA has engaged regulators, including the Securities and Exchange Commission ("**SEC**") and Commodity Futures Trading Commission ("**CFTC**"), on the issue of data security and treatment of confidential information. We provide below some of our concerns and recommendations for the Senate Banking Committee's consideration, focusing on recommendations we've made to the SEC.

I. Background

MFA and its members have strong concerns about information security at regulatory agencies. Information security vulnerabilities at a regulator jeopardize not only market participants and their investors, but the U.S. economy through the loss of domestic trade secrets and confidence in the integrity of the regulatory framework.[3] Over the last several years, due to both statutory mandates and regulatory

[1] 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 over time. MFA has cultivated a global membership and actively engages with regulators and policymakers in Asia, Europe, North and South America, and many other regions where MFA members are market participants.

[2] Crapo, Brown Invite Feedback on Data Privacy, Protection and Collection, February 13, 2019, available at: https://www.banking.senate.gov/newsroom/majority/crapo-brown-invite-feedback-on-data-privacy-protection-and-collection.

[3] *See* Gregory C. Wilshusen, Director, Information Security Issues, Testimony before the Subcommittee on Research and Technology Oversight, Committee on Science, Space, and Technology, House of Representatives, 7 (July 8, 2015), (GAO reporting that federal agencies had 77,183 cybersecurity incidents in 2015 along—a 1,300% increase since 2006) available at: http://www.gao.gov/assets/680/670935.pdf. In addition, the list of recent federal government cyber breaches is long and growing, including the Central Intelligence Agency, White House, Department of State,

discretion, agencies have expanded the scope and breadth of the types of information that they request of registrants. They have, however, generally continued to rely on the same frameworks for information collection and protection.

II. SEC Data Collection & Recommendations for Protection

A. Scope of Data Collection

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 may request 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 SEC'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. MFA appreciates the steps SEC Chairman Jay Clayton has taken with respect to data protection and supports continued prioritization and vigilance in this area.[5] Current statutory provisions designed to protect the confidential and proprietary information of registrant will be ineffective though unless the SEC has robust, updated policies and procedures to implement statutory requirements.[6]

Federal Deposit Insurance Corporation, Federal Aviation Administration, Department of Defense, Internal Revenue Service, Office of Personnel Management, the Pentagon, the Federal Reserve, Department of Homeland Security, Federal Bureau of Investigation and Department of Treasury. *See* Continued Federal Cyber Breaches in 2015, Riley Walters, Nov. 19, 2015, available at: http://www.heritage.org/research/reports/2015/11/continued-federal-cyber-breaches-in-2015; The IRS Says Identity Thieves Hacked Its Systems Again, Fortune, Feb. 10, 2016, available at: http://fortune.com/2016/02/10/irs-hack-refunds/; Federal Reserve Hacked More than 50 Times in 4 Years, The Huffington Post, June 1, 2016, available at: http://www.huffingtonpost.com/entry/hackers-breach-federal-reserve-50-times_us_574ee0d5e4b0757eaeb1194c; Republican Staff Memorandum to Republican Members, Committee on Science, Space and Technology, July 12, 2016 available at: https://www.documentcloud.org/documents/2992789-Final-GOP-Interim-Staff-Report-7-12-16.html; Lorenzo Franceschi-Bicchierai, "Hacker Publishes Personal Info of 20,000 FBI Agents," Motherboard, February 8, 2016, available at: https://motherboard.vice.com/read/hacker-publishes-personal-info-of-20000-fbi-agents; and News release, "OCC Notifies Congress of Incident Involving Unauthorized Removal of Information," U.S. Department of the Treasury, Office of the Comptroller of the Currency, October 28, 2016, available at: http://www2.occ.gov/news-issuances/news-releases/2016/nr-occ-2016-138.html.

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

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

[6] *See,* Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551 (2014); Section 404 of the Dodd-Frank Act; 18 U.S.C. § 654 (1996) (prohibiting an officer of employee of United States converting property of another); *and* 18 U.S.C. § 1905 (2008) (prohibiting public officers and employees of disclosure of confidential information generally). *See also* Fiscal Year 2018 Independent Evaluation of SEC's Implementation of the Federal Information Security Modernization Act of 2014, SEC Office of Inspector General, December 17, 2018, (reporting that the SEC's information security program was ineffective under the *FY 2018 IG FISMA Reporting Metrics*) available at: https://www.sec.gov/files/FY-2018-Independent-Eval-SEC-Implementation-of-the-FISMA-of-2014-Report-No-552.pdf; Evaluation of the EDGAR System's Governance and Incident Handling Processes, SEC Office of the Inspector General, September 21, 2018, (finding that the EDGAR system lacked adequate governance commensurate with the system's importance to the SEC's mission, certain preventive controls either did not exist or operate as designed, and the SEC lacked an effective incident handling process), available at: https://www.sec.gov/files/Eval-of-the-EDGAR-Systems-Governance-and-Incident-Handling-Processes.pdf; Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2017, SEC Office of the Inspector General, March 30, 2018, (finding that the SEC's information security program was ineffective under

Recommendation #1: As part of the SEC's strategy to mitigate systemic risk and harm to investors and registrants from cyber theft, we recommend that the SEC institutionalize the practice of tailoring its data requests to that which is necessary to achieve its core mission. The SEC should limit the scope of systemic risk filings to information that could reasonably identify such risks and exam requests to data that is necessary to ensure compliance. To assist the SEC with this request, MFA developed recommendations for revising Form PF to rationalize and simplify reporting.[7]

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

It is MFA's position that the SEC must have the requisite information to oversee registrants and to surveil markets. In the past, MFA has expressed concern that SEC staff, at times, unnecessarily requested access to highly confidential and commercially-valuable intellectual property, without exhausting other less sensitive means of understanding a firm's activities, and then did not have robust procedures for protecting such information. The SEC's oversight authority needs to be exercised with consideration for the potential risk of irrevocable harm to registrants and their investors (*e.g.*, unauthorized disclosure or misappropriation of trade secrets).

While the Dodd-Frank Act imposed heightened confidentiality protections with respect to systemic risk information that the SEC collects from managers of private funds,[8] we think regulators should impose heightened procedures and standards with respect to all highly sensitive and confidential information that they receive regardless of how it is collected. If the SEC collects highly confidential and commercially-valuable intellectual property from registrants, we think it should consider emulating industry practices and standards with respect to protecting confidential intellectual property. Market participants go to great lengths to protect sensitive intellectual property, implementing practices shaped by case law from intellectual property cases. We think it is only appropriate for the SEC to apply consistent protections.

Recommendation #2: MFA recommends that the SEC incorporate protections within the design of its forms and reporting systems to mitigate cyber breaches. The SEC should enable investment advisers to use an alphanumeric identifier for filings, to be kept separately within the SEC systems, and limit

---

the *FY 2017 IG FISMA Reporting Metrics*), available at: https://www.sec.gov/files/Audit-of-the-SECs-Compliance-with-FISMA-for-Fiscal-Year-2017.pdf; Office of Management and Budget, Annual Report to Congress on the Federal Information Security Modernization Act of 2014, Fiscal Year 2016 (reporting that the SEC's information security program was ineffective under the FY 2016 Inspector General FISMA Reporting Metrics) available at: https://www.whitehouse.gov/sites/whitehouse.gov/files/briefing-room/presidential-actions/related-omb-material/fy_2016_fisma_report%20to_congress_official_release_march_10_2017.pdf; Office of Inspector General, SEC, Audit of the SEC's Compliance with the Federal Information Security Modernization Act for Fiscal Year 2015, June 2, 2016, Rep. No. 535, (urging SEC management to take certain actions to address potential risk with respect to the SEC's information security program) available at: https://www.sec.gov/oig/reportspubs/Audit-of-the-SECs-Compliance-with-the-Federal-Information-Security-Modernization-Act-for-Fiscal-Year-2015.pdf; *and* U.S. GAO Report to the Chair, U.S. SEC, on Information Security "Opportunities Exist for SEC to Improve its Controls over Financial Systems and Data," April 2016, (finding that the SEC needs to improve its controls over financial systems and data as weaknesses continue to limit the effectiveness of security controls) available at: http://www.gao.gov/assets/680/676876.pdf.

[7] *See* letter from the Honorable Richard H. Baker, President and CEO, MFA, and Jennifer W. Han, Associate General Counsel, MFA, dated September 17, 2018, on "A Streamlined Form PF: Reducing Regulatory Burdens", available at: https://www.managedfunds.org/wp-content/uploads/2018/09/MFA.Form-PF-Recommendations.attachment.final_.9.17.18.pdf.

[8] *See* Section 404 of the Dodd-Frank Act.

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, MFA recommends that the SEC exam staff implement a process through which it would exhaust 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 necessary and execute those requests through the subpoena process. Further, we recommend that the SEC adopt 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. Legislative Measures

MFA believes that the Senate Banking Committee should also consider legislative solutions with respect to enhancing data privacy, protection and collection. During the 115th Congress, Senator David Purdue introduced **S.3733, the "Protection of Source Code Act**," which would amend the securities statutes to require the SEC to issue a subpoena before compelling a person to "produce or furnish source code, including algorithmic trading source code or similar intellectual property that forms the basis for design of the source code." Senator Purdue also introduced S.3732, that would apply the same scheme proposed for the SEC in the "Protection of Source Code Act" to the CFTC through changes to the Commodity Exchange Act. Similar legislation (HR 3948, the "Protection of Source Code Act") was introduced in the House of Representatives in the 115th Congress by Representative Sean Duffy (WI) and cosponsored by Representative David Scott (GA) and others, and received broad bipartisan support in the House Committee on Financial Services.

MFA believes that legislation such as the Protection of Source Code Act and companion House bill would be an important and constructive step for implementing and ensuring that regulators have a robust process in place when it comes to determining the necessity of highly sensitive, confidential information. Significantly, the legislative measure does not impede regulators from seeking the information they need, it only ensures that regulators have a process in place before seeking certain types of information, balancing the needs of regulators and registrants. As such, MFA supports the policy of the "Protection of Source Code Act" and recommends that the Senate Banking Committee consider such legislation during this Congress.

* * * * *

MFA appreciates your request for feedback on data privacy, protection and collection. MFA is committed to working with Members and staff of Congress, the Committee, regulators, and all interested parties to enhance data protection. We would be pleased to discuss our views and comments further with you, the Banking Committee and its staff.

Respectfully submitted,

/s/ Richard H. Baker

Richard H. Baker
President and CEO