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

Recommendations for FSOC Members/Regulators
On the Protection of Non-public, Sensitive and Proprietary Information
May 2013

I. Introduction & Summary

Managed Funds Association[1] ("**MFA**") wishes to express concern to the Financial Stability Oversight Council ("**FSOC**") and its member agencies'[2] ("**Regulators**") regarding their protection of non-public, sensitive and proprietary information collected or shared as part of a Regulator's oversight of financial market participants and/or financial stability.[3] Regulators, in the course of discharging their various responsibilities under the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 ("**Dodd-Frank Act**"), are collecting an unprecedented level and quantity of non-public, sensitive and proprietary information concerning investment

[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, the Americas, Australia and many other regions where MFA members are market participants.

[2] FSOC Member Agencies are: the Department of the Treasury, the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Bureau of Consumer Financial Protection, the Securities and Exchange Commission, the Federal Deposit Insurance Corporation, the Commodity Futures Trading Commission, the Federal Housing Finance Agency, the National Credit Union Administration, the Office of Financial Research, and the Federal Insurance Office; as well as individual FSOC Members, such as the independent Presidential appointee, the designated state insurance commissioner, the designated state banking supervisor, and the designated state securities commissioner.

Our recommendations herein on the protection of non-public, sensitive and proprietary information apply to all FSOC member and member agencies, voting and non-voting members alike to the extent a member or member agency receives non-public, sensitive and proprietary information. For example, the Director of the Office of Financial Research ("**OFR**") is a non-voting member, but as OFR is in a position to access and even collect sensitive and proprietary information it must ensure that it is protecting sensitive and proprietary information as fully as possible.

[3] *See, e.g.,* Audit of the Financial Stability Oversight Council's Controls over Non-public Information, The Council of Inspectors General on Financial Oversight, June 2012; Semiannual Report for CFTC, CFTC Office of Inspector General, Oct. 31, 2012; SEC's Controls over Sensitive/Nonpublic Information Collected and Exchanged with the Financial Stability Oversight Council and Office of Financial Research, SEC Office of Inspector General, Mar. 25, 2013; 2012 FISMA Executive Summary Report, SEC Office of Inspector General, Mar. 29, 2013; *Academic Use of CFTC's Private Derivatives Data Investigated,* Bloomberg, Mar. 7 2013; *CME Group sparked shutdown of CFTC's academic research program,* Reuters, April 24, 2013; and *SEC needs better controls to protect data – watchdog,* Reuters, Apr. 3, 2013.

strategies from market participants.[4] MFA broadly supports such data collection efforts to inform policy making, but believe FSOC and Regulators need to ensure that they are protecting the data as fully as possible.

Market participants invest significant research, time and resources into developing proprietary investment strategies. Such investment strategies are trade secrets, protected by law. The Dodd-Frank Act, like other statutes,[5] recognizes the legitimate commercial need to protect the confidentiality of such secrets; and sets forth confidentiality and information-sharing provisions among the Regulators. We also believe that as a matter of financial stability, it is important for Regulators to maintain the confidentiality of market participants' trade data and investment strategies. We are concerned that if FSOC or Regulators disclose sensitive or proprietary information relating to an investment firm's portfolio or investment, recipients could use such information to trade against the investment firm and cause, especially during times of market stress or financial stress for the investment firm, further market or financial stress, and even the potential liquidation of such firm's fund or positions. Moreover, recipients of such information might be able to employ the data in ways that could be harmful more broadly.

In light of recent inspector general reports, press reports and Regulators' new Dodd-Frank Act authorities and information-sharing duties and obligations, MFA believes it is appropriate and necessary for Regulators to review their existing policies, practices and controls now before either a Regulator inadvertently leaks information or a hacker perpetrates a malicious attack. We urge FSOC and the Regulators to coordinate such a review of practices and controls with fellow FSOC members and to address any necessary concerns or weakness that the review reveals.[6] To that end, MFA has developed a number of recommendations for the Commodity Futures Trading Commission ("**CFTC**") and the Securities and Exchange Commission ("**SEC**", with the CFTC, the "**Commissions**"), as the primary regulators of investment advisers/pool operators and their funds, and the FSOC and its members, as the collective financial stability regulators, to strengthen policies and controls around the protection of non-public information. While we address certain recommendations to the Commissions in response to specific events, we believe the recommendations may be broadly applicable to Regulators.

Discussed in detail below, MFA makes the following recommendations:

1. MFA recommends that the Commissions review and harmonize policies and controls concerning the treatment of sensitive and proprietary information.

---

[4] *See* Section 112 of the Dodd-Frank Act (requiring the FSOC to collect information from member agencies to assess systemic risk). MFA supported enhanced information reporting during the legislative process that resulted in the enactment of the Dodd-Frank Act. *See* Testimony of the Honorable Richard H. Baker, before the Committee on Financial Services, U.S. House of Representatives, October 29, 2009, available at: http://www.managedfunds.org/downloads/MFA%20Written%20Testimony.pdf.

[5] *See e.g.*, Freedom of Information Act, 5 USC §552 (b)(4) (hereinafter "FOIA") (exception for "trade secrets and commercial or financial information obtained from a person and privileged or confidential….").

[6] *See* Section 112 of the Dodd-Frank Act. *See supra* n. 2.

2. MFA recommends that Regulators review the robustness of their policies, practices and controls relating to their use and treatment of sensitive and proprietary information and adopt such enhancements as are necessary.

3. MFA recommends that Regulators heighten staff sensitivity and awareness on the handling of non-public, sensitive and proprietary information through annual trainings and certifications, and regular reminders.

4. MFA recommends that FSOC Member Agencies implement a uniform system for sharing and protecting non-public information; such uniform system should include detailed controls and procedures around the access, documentation and use of non-public information, and be tailored appropriately for the level of sensitivity of the information.

5. MFA recommends that the Commissions require and confirm that Data Repositories and other regulated entities maintain robust policies, practices and controls to protect the confidentiality of sensitive and proprietary information, including the identity of traders and the nature of their trading activities.

II. Preventing the Misuse of Sensitive and Proprietary Information

A. Harmonizing Policies and Controls at the CFTC and SEC

MFA believes that the Commissions should harmonize their policies and controls around the treatment of private, sensitive data collected for regulatory purposes as fully as possible. The Commissions share the most overlap of regulated entities and policies, and as a result, have the greatest need for cooperation. We recognize that there are discrepancies between the Commodity Exchange Act ("**CEA**") and the securities laws with respect to the treatment of non-public, sensitive and proprietary data, information and/or materials (referred to herein as "sensitive and proprietary information"). Nevertheless, these federal laws share an objective, *i.e.*, the protection of sensitive and proprietary information. As the Commissions are both regularly in receipt of sensitive trade data, and collect substantially the same information from investment advisers, commodity pool operators and commodity trading advisors; and foreseeably will be collaborating in investigations (*i.e.*, the CFTC and SEC staffs' joint report on the May 6, 2010 market event[7]) and sharing and exchanging sensitive and proprietary information, we believe the Commissions should harmonize their policies and controls with respect to the treatment of sensitive and proprietary information.

Generally, although not exclusively, the Commissions receive sensitive and proprietary information of investment advisers, commodity pool operators ("**CPOs**"), commodity trading advisors ("**CTAs**") and their funds from the following sources: trade data from self-regulatory organizations, intermediaries and other regulated entities (*i.e.*, broker-dealers, futures commission merchants, swap data repositories and clearinghouses); new systemic risk reports

[7] *See* Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues, *Findings Regarding the Market Events of May 6, 2010*, September 30, 2010, available at: http://www.cftc.gov/ucm/groups/public/@otherif/documents/ifdocs/staff-findings050610.pdf.

(*i.e.*, Forms PF, CPO-PQR, and CTA-PR); and examinations. Regardless of how the Commissions obtain the sensitive and proprietary information, we believe that the Commissions must have robust policies and controls to protect such information in accordance with law.[8]

Congress has directed both Commissions to protect confidential information. Section 8(a) of the CEA provides that the CFTC "may not publish data and information that would separately disclose the business transactions or market positions of any person and trade secrets or names of customers."[9] (*See* **Appendix A** for the full language.)

Similarly, Section 24(b) of the Securities Exchange Act of 1934 ("**Exchange Act**") provides that a "member, officer, or employee" of the SEC is prohibited from "disclos[ing] to any person other than a member, officer, or employee of the [SEC], or to use for personal benefit, any information" protected under section 552 of Title 5 of the U.S. Code or SEC regulations.[10] Section 204(b) of the Investment Advisers Act of 1940 ("**Advisers Act**") provides that "any proprietary information of an investment adviser ascertained by the [SEC] from any report required to be filed with the [SEC] . . . shall be subject to the same limitations on public disclosure as any facts ascertained during an examination;"[11] and that any other regulatory entity that receives such proprietary information from the SEC "shall maintain the confidentiality of such reports, documents, records, and information in a manner consistent with the level of confidentiality established" by the SEC.[12] (See **Appendix A** for the full language.)

Pursuant to Sections 112 and 404 of the Dodd-Frank Act and Section 1a of the CEA, the Commissions adopted new rules requiring SEC-registered investment advisers, and CFTC-registered CPOs and CTAs to file systemic risk reports—respectively, Form PF, Form CPO-PQR, and Form CTA-PR (together "**Systemic Risk Reports**").[13] The Commissions allow a registrant that is both an SEC-registered investment adviser and a CFTC-registered CPO or CTA to file Form PF to satisfy as "substituted compliance" certain filing obligations under Form CPO-PQR and CTA-PR.[14]

We believe it makes practical sense for the Commissions to harmonize their policies and controls around the treatment of sensitive and proprietary information for several reasons. First, in order for the CFTC to receive proprietary investment adviser information from the SEC, the

---

[8] *See* Section 8(a) of the Commodity Exchange Act ("CEA"); Section 24 of the Securities Exchange Act of 1934 ("Exchange Act"); Section 204 of the Investment Advisers Act of 1940 ("Advisers Act"); FOIA *supra* n. 5; and Section 112(b)(5) of the Dodd-Frank Act.

[9] Section 8(a)(1) of the CEA.

[10] Section 24 of the Exchange Act. *See also*, FOIA *supra* n. 5.

[11] Section 204(b)(10) of the Advisers Act.

[12] Section 204(b)(9) of the Advisers Act.

[13] *See* 76 Fed.Reg. 71128 (Nov. 16, 2011), Reporting by Investment Advisers to Private Funds and Certain Commodity Pool Operators and Commodity Trading Advisors on Form PF, available at: http://www.gpo.gov/fdsys/pkg/FR-2011-11-16/pdf/2011-28549.pdf; and 77 Fed. Reg. 11252 (Feb. 24, 2012), Commodity Pool Operators and Commodity Trading Advisors: Compliance Obligations, available at: http://www.cftc.gov/ucm/groups/public/@lrfederalregister/documents/file/2012-3390a.pdf.

[14] *See id.*

Dodd-Frank Act requires that the receiving agency must maintain the confidentiality of such information in a manner consistent with the level of confidentiality established at the SEC.[15] To do so, the CFTC must have comparable policies and controls in place as the SEC to protect confidential information. Nevertheless, to the extent the CFTC receives freedom of information requests with respect to sensitive and proprietary information it has received from the SEC, we believe the CFTC as the receiving agency should defer to the SEC on its policies and procedures. Second, as the markets the Commissions oversee become ever more intertwined, it is reasonably foreseeable that the Commissions will engage in a greater number of joint investigations, and frequent sharing of sensitive and proprietary information. Finally, we believe that if the Commissions harmonize their policies and controls on the treatment of sensitive and proprietary information, it may reduce the likelihood of inadvertent disclosures of sensitive and proprietary information. Accordingly, we recommend that the Commissions review and harmonize policies and controls around the treatment of sensitive and proprietary information.

Recommendation: MFA recommends that the Commissions review and harmonize policies and controls concerning the treatment of sensitive and proprietary information.

B. Enhancing Policies and Controls to Protect Sensitive and Proprietary Information

MFA believes that the Commissions should update and enhance the robustness of their policies, practices and controls around the use and treatment of sensitive and proprietary information. The Dodd-Frank Act bestows upon the Commissions, in their new role to oversee financial stability, new authorities to collect and share information.[16] As the Commissions are collecting on a routine basis an unprecedented level of sensitive and proprietary information, we believe they need to ensure that they have robust policies and controls around the collection and handling of sensitive and proprietary information (*e.g.*, Forms PF, CPO-PQR and CTA-PR). We are concerned from recent press and inspector general reports that the Commissions do not have adequate policies, practices and controls to protect the confidentiality of sensitive and proprietary information.

The Commissions require investment advisers, CPOs and CTAs to file Systemic Risk Reports.[17] These reports require Registrants to report highly sensitive and proprietary information relating to their businesses through these Systemic Risk Reports, including investment holdings. As discussed above, Section 8(a) of the CEA and Section 204(b) of the Advisers Act require that the Commissions protect the confidentiality of an investment adviser's, CPO's and CTA's sensitive and proprietary information.[18]

---

[15] Section 404 of the Dodd-Frank Act (amending Section 204(b) of the Advisers Act).

[16] Section 112 of the Dodd-Frank Act

[17] *See supra* n. 13.

[18] *See supra* n. 9-12 and corresponding text.

We are extremely concerned with recent findings in the SEC Inspector General report on "controls over sensitive/nonpublic information collected and exchanged with the FSOC and OFR" ("**Report on Controls over Sensitive/Nonpublic Information**").[19] The Report on Controls over Sensitive/Nonpublic Information concludes that the SEC has insufficient controls to protect the data collected through the Form PF process. Specifically, it found that: (1) the lack of remote access controls may put sensitive and nonpublic information at risk of unauthorized disclosure;[20] (2) the SEC's protocol for inventorying, tracking, and marking information collected by and exchanged with FSOC, its Member Agencies, and OFR needs improvement;[21] and (3) new contractors are not provided training on handling sensitive and nonpublic information in a timely manner.[22]

Similarly, we are extremely troubled and alarmed by recent press reports alleging that CFTC staff and outside researchers used sensitive and proprietary information and published independent research papers based on that information that were not sanctioned by the CFTC.[23] First, as such data is protected from disclosure by law we are concerned that non-CFTC staff had access to it.[24] Second, we are concerned that certain CFTC staff and non-CFTC staff may have reverse-engineered certain trading strategies and published information that should be regarded as trade secrets, business transactions or commercial or financial information. Even though the research papers did not reveal the identities of traders, they revealed trade secrets and commercial or financial information in direct violation of federal laws.[25] Also, the research papers seem to indicate that the researchers had access to proprietary information that they could have used for other purposes, such as trading against a market participant (*e.g.*, front running) or "cloning" a market participant's profitable trading strategies. Finally, we are concerned that papers based on highly sensitive and confidential information were not submitted to the CFTC Commission members or separate staff for approval prior to publication.

We strongly believe that the Commissions need to have comprehensive internal policies and controls implementing the mandates of the federal statutes mentioned above, to prohibit and

---

[19] *See* SEC's Controls over Sensitive/Nonpublic Information Collected and Exchanged with the Financial Stability Oversight Council and Office of Financial Research, SEC Office of Inspector General, Mar. 25, 2013.

[20] The Report on Controls over Sensitive/Nonpublic Information found that SEC employees and contractors remotely accessing SEC's email system are not restricted from saving and uploading sensitive or nonpublic information on non-SEC computers.

[21] The Report on Controls over Sensitive/Nonpublic Information found that the SEC had not appointed a primary information owner to oversee information the SEC receives and shares with FSOC, its Member Agencies, or OFR; and that a protocol for inventorying and ensuring that information is appropriately marked had not been fully developed.

[22] The Report on Controls over Sensitive/Nonpublic Information found that newly assigned contractors working with FSOC, its Member Agencies, and the OFR information are not promptly and adequately trained on how to handle sensitive or nonpublic information.

[23] *See, e.g.,* Adam Clark-Joseph, *Exploratory Trading*, January 13, 2013. *See also,* Andrei Kirilenko et al., *The Flash Crash: The Impact of High Frequency Trading on an Electronic Market*, May 26, 2011; and Jaksa Cvitanic and Andrei Kirilenko, *High Frequency Traders and Asset Prices*, March 11, 2010.

[24] *See* Section 8(a) of the Commodity Exchange Act.

[25] *See supra* n. 23 and *supra* n. 8.

prevent the misuse or disclosure of sensitive and proprietary information. The Commissions should consider such policies and controls in conjunction with their requirements under the Federal Information Security Management Act of 2002[26] ("**FISMA**"), and the standards set by the National Institute of Standards and Technology ("**NIST**") in connection with FISMA.[27] (See **Appendix B** for NIST criteria for an effective information security program.) We believe NIST Special Publication 800-53 sets forth a very useful set of security and privacy controls, specifically developed to help protect federal information systems and organizations.[28] We recommend that the Commissions consider the latest standards set forth by NIST in revising its internal policies, practices and controls around sensitive and proprietary information.

At a minimum, such policies and controls to prevent the disclosure of non-public information should outline appropriate use of sensitive and proprietary information and prohibit the publication of any report that has the potential of exposing the identity of specific market participants, or that would harm market participants or legitimate trading strategies even without disclosure of the identities of such market participants. Examples of the types of policies and controls that the Commissions should include, but are not limited to policies and controls that:

- Limit internal access to sensitive and proprietary information to relevant staff and employees;
- Log staff/employee and contractor access to databases with sensitive and proprietary information;
- Password protect files with sensitive information;
- Monitor when data is downloaded or transferred;
- Restrict the ability to download, transfer or save sensitive non-public information to a non-government computer, storage device or portable or removable media;
- Require periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually;[29]
- Implement procedures for detecting, reporting (*i.e.*, to the owner of the information), and responding to the improper use of nonpublic information;
- Implement a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization;[30]
- Require periodic third party testing and evaluation of policies, practices and controls around the protection of sensitive and proprietary information; and

---

[26] Title III of the E-Government Act of 2002, Pub. L. 107-347 (2002) (recognizing the importance of information security to the economic and national security interests of the United States). FISMA requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency.

[27] *See* FISMA Implementation Project on the NIST website, available at: http://csrc.nist.gov/groups/SMA/fisma/index.html.

[28] *See* Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 (April 2013), available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[29] This is a NIST recommendation for an effective security program. *See id.*

[30] This is a NIST recommendation for an effective security program. *See id.*

- Impose disciplinary action for improper use of confidential data.

We believe the Commissions should also consider retaining an outside expert in data security to work with staff to design robust protections and internal controls.

In general, we are wary of the Commissions providing third parties, including consultants and academic researchers, access to confidential data or materials from which market participants may be identified or their strategies revealed. Even with non-disclosure agreements in place, we believe it can be challenging to monitor whether third parties abide by such agreements and do not misappropriate or use any information for improper purposes. Congress authorized the Commissions to collect sensitive and proprietary information "as necessary and appropriate in the public interest and for the protection of investors, or for the assessment of systemic risk."[31] Accordingly, we believe such sensitive and proprietary information should only be used for essential regulatory oversight functions. To the extent that the Commissions provide third parties with access to confidential materials, including the ability to read or study such materials, we believe they should have robust policies and controls in place, which at a minimum:

- Require a third party to sign a confidentiality and non-disclosure agreement;
- Limit and control the information provided to a third party;
- Specifically outlines the purpose and scope of allowed use of the materials;
- Document all persons with access to sensitive and proprietary information and the reason for their access to such information;
- Limit the use of sensitive and proprietary information for purposes that are in the public interest and for the protection of investors or for the assessment of systemic risk;
- Require a cost-benefit assessment, and documentation of such assessment, when sensitive and proprietary information is used for the purposes of a "study";
- Require Commission approval for the publication of a study based on sensitive and confidential information;
- Mask the identity of market participants or remove identifying information;
- Control access to the confidential information;
- Implement a mechanism for reporting the improper use of sensitive and proprietary information; and
- Impose disciplinary action for improper use of sensitive and proprietary information.

We also respectfully urge the Regulators to examine their protections against third party "hack" attacks. President Obama has declared cyber threat as one of the most serious economic and national security challenges, directing a full review of the Federal Government's efforts to defend its information and communications infrastructure.[32] Similarly, Department of Treasury officials have spoken of the Department's concerns with cyber-attacks on the Federal

[31] *See* Section 204(b) of the Advisers Act. *See also* Section 8(a) of the CEA (providing that the CFTC "may publish from time to time the results of . . . such general statistical information gathered therefrom as it deems of interest to the public" provided that it doesn't disclose trade secrets).

[32] Remarks by the President on Securing Our Nation's Cyber Infrastructure, The White House, May 29, 2009, available at: http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure.

Government and key financial institutions.[33] Regulators must secure vital, proprietary information they receive from market participants from such cyber security attacks. The Regulators correctly impose obligations on market participants, such as the recent identity theft rules, to protect sensitive investor and client information.[34] Similarly, Regulators should have protections in place to secure sensitive and proprietary information they receive from registrants and market participants to protect investor and client information.

Of course, as a private sector entity, MFA has no specific knowledge of Regulators' existing capabilities to protect against cyber-attacks. We presume that the Regulators are well aware of these threats and have taken meaningful action to protect the information that they hold. Nonetheless, with the ever increasing threat of hacking and other illegal behavior in addition to Regulators' increasing demand for sensitive and proprietary data from market participants, we believe it is important to ensure that the Regulators are taking all reasonable precautions. Accordingly, we recommend that Regulators review the robustness of their policies, practices and controls relating to their use and treatment of sensitive and proprietary information and adopt such enhancements as are necessary.

Recommendation: MFA recommends that Regulators review the robustness of their policies, practices and controls relating to their use and treatment of sensitive and proprietary information and adopt such enhancements as are necessary.

C. Staff Training on Policies and Controls

MFA believes that Regulators should require annual security awareness training to inform personnel of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks.[35] MFA presumes that Regulators have general policies and procedures in place with respect to handling non-public information, including information learned in the ordinary course of performing regulatory functions. Pursuant to rulemaking implementing the Dodd-Frank Act, we believe many new personnel at Regulators may now have responsibility working with sensitive and proprietary information—information that should be held to a higher level of protection and restriction than simply non-public information learned in the ordinary course of business. For example, we believe that staff in rulemaking offices or divisions, or staff assigned to FSOC projects, who previously may not have worked with sensitive and proprietary information, should be trained and certified on policies and controls around sensitive and

---

[33] *See* U.S. Presses on Cyberthreats, W.S.J., March 20, 2013, available at: http://online.wsj.com/article/SB10001424127887324373204578372132763639230.html; Remarks of Secretary Jacob J. Lew at Johns Hopkins University School of Advanced International Studies, April 17, 2013, available at: http://www.treasury.gov/press-center/press-releases/Pages/jl1899.aspx. *See also* FSOC 2013 Annual Report, April 25, 2013, available at: http://www.treasury.gov/initiatives/fsoc/Documents/FSOC%202013%20Annual%20Report.pdf.

[34] 78 Fed.Reg. 23638 (April 19, 2013), Identity Theft Red Flags Rule, available at: http://www.gpo.gov/fdsys/pkg/FR-2013-04-19/pdf/2013-08830.pdf (requiring certain SEC or CFTC registrants to implement identity theft red flags policies and procedures).

[35] *See* **Appendix** B for NIST recommendations for an effective security program.

proprietary information prior to assuming regulatory responsibilities involving sensitive and proprietary information. If not currently doing so, we recommend that Regulators heighten staff sensitivity and awareness on the handling of sensitive and proprietary information through annual trainings and certifications, and regular reminders.

Recommendation: MFA recommends that Regulators heighten staff sensitivity and awareness on the handling of non-public, sensitive and proprietary information through annual trainings and certifications, and regular reminders.

D. Coordinating Policies and Controls Among FSOC Member Agencies

MFA believes that FSOC Member Agencies should review and coordinate their policies, practices and controls around the sharing of sensitive and proprietary information. We are concerned that differences in policies and practices at FSOC Member Agencies may lead to the inadvertent disclosure of sensitive and proprietary information. Further, we believe that coordinated policies and practices around the sharing of sensitive and proprietary information will help strengthen controls at FSOC Member Agencies and OFR.

The Dodd-Frank Act requires members of FSOC to "collect information from member agencies . . . to assess risks to the United States financial system"[36] as well as to "maintain the confidentiality of any data, information, and reports" received pursuant to the Financial Stability Act.[37] While members of FSOC have each signed the *Memorandum of Understanding Regarding the Treatment of Non-public Information Shared Among Parties Pursuant to the Dodd-Frank Act*, we are concerned that differences in each member's policies and controls may lead to inadvertent breaches of information security.[38]

For example, the Council of Inspectors General on Financial Oversight ("**CIGFO**") found that FSOC members have different marking systems for designating non-public information and different controls for handling non-public information.[39] We support CIGFO's suggestion that FSOC Member Agencies "further examine the issues raised in [CIGFO's audit report of FSOC] to increase their understanding of the differences in members' information control environments" and develop best practices.[40] We also agree on the importance of FSOC members acting in a timely manner with regard to developing tools for secure collaboration and controlled access to data shared among FSOC members, considering the potential heightened impact designation of new information and the control ramifications of decisions made about such information.[41]

---

[36] Section 112(a)(2) of the Dodd-Frank Act.

[37] Section 112(d)(5) of the Dodd-Frank Act.

[38] *See, e.g., Audit of the Financial Stability Oversight Council's Controls over Non-public Information*, Report to FSOC and the Congress, prepared by The Council of Inspectors General on Financial Oversight (June 2012).

[39] *See id.*

[40] *Id.*

[41] *Id.*

We recommend that FSOC Member Agencies implement a uniform system for sharing and protecting non-public information. Such uniform system should include detailed controls and procedures around the access, documentation and use of non-public information (*see, e.g.,* section I.B. above); and tailored appropriately for the level of sensitivity of the information. While our specific discussion in section I.B. was directed at the Commissions, we believe the recommendations are relevant for all FSOC Member Agencies, especially as the Advisers Act requires any other regulatory entity that receives investment adviser reports to maintain the confidentiality of such reports in a manner consistent with the SEC.[42] We commend CIGFO for creating a working group to evaluate FSOC controls over non-public information and the manner in which FSOC and Member Agencies safeguard information from unauthorized disclosure.[43] We believe this working group will be very helpful in enhancing FSOC and its members' policies and controls with respect to non-public information.

Recommendation: MFA recommends that FSOC Member Agencies implement a uniform system for sharing and protecting non-public information; such uniform system should include detailed controls and procedures around the access, documentation and use of non-public information, and be tailored appropriately for the level of sensitivity of the information.

III. Protecting Sensitive & Proprietary Information at Regulated Entities

We believe that the Commissions should clarify that under final rules relating to swap data repositories ("**SDRs**") and security-based swap data repositories ("**SBSDRs**") (together, "**Data Repositories**"), Data Repositories, as part of their obligations to maintain the privacy of transaction information,[44] must have robust policies and controls to protect both the identity of traders and sensitive and proprietary information. We believe the Commissions should also remind other industry market utilities, such as self-regulatory organizations, designated contract markets, designated clearing organizations or clearinghouses ("**Regulated Entities**"), of their obligation to maintain the privacy of transaction information. Specifically, we would like to ensure that as new Data Repositories establish their policies, practices and controls, they and Regulated Entities implement robust confidentiality protections that: (1) protect counterparty anonymity for transactions at all times;[45] and (2) protect against inadvertent disclosure of trade data. We respectfully urge the Commissions in their oversight roles to review the policies,

---

[42] *See supra* n. 12 and corresponding text. We note that the SEC requests for comments on proposed rules concerning the sharing of security-based swap data by a SBSDR and a foreign regulatory entity. *See* Cross-Border Security-Based Swap Activities; Re-Proposal of Regulation SBSR and Certain Rules and Forms Relating to the Registration of Security-Based Swap Dealers and Major Security-Based Swap Participants, Exchange Act Release No. 34-69490 (May 1, 2013). We believe that the SEC and/or the SBSDR, prior to providing a foreign regulatory entity with security-based swap data, should seek assurances that such foreign regulatory entity will maintain the confidentiality of such data in a manner consistent with the SEC and/or SBSDR.

[43] Annual Report of the Council of Inspectors General on Financial Oversight, July 2012.

[44] *See, e.g.,* Sections 728 and 763(i) of the Dodd-Frank Act.

[45] *See* letter from Stuart J. Kaswell, Executive Vice President & Managing Director, MFA, to Richard A. Shilts, Director, CFTC, dated February 28, 2013, regarding a "Request for Interpretive Guidance – Swap Counterparty Access to Legal Entity Identifiers in SDR Data and Information."

practices and controls at Data Repositories with respect to the protection of sensitive and proprietary information.

Regarding the protection of counterparty anonymity, we understand, for example, that as an exception to the requirement to protect the confidentiality of reported swap data, an SDR may provide a party to a particular swap access to "data and information" related to such swap.[46] While "data and information" have not been defined, we believe CFTC and SEC regulations a should strictly prohibit a Data Repository from disclosing information to other market participants that would reveal the identity of traders, including through legal entity identifiers or other information, products traded, or the nature of their trading activities.

A key element to ensuring the market's confidence is to ensure that Data Repositories have robust systems and processes for the protection of confidential data. We are concerned by recent instances where a data repository inadvertently exposed confidential trade data. It is important for Data Repositories to implement appropriate policies and controls to prevent the inadvertent disclosure of sensitive and proprietary information. Such policies should also include protocols to mitigate and contain the harm when confidential information is disclosed and certain escalation and reporting procedures whereby the Data Repositories would immediately notify regulators and affected market participants. Furthermore, Data Repositories need policies and procedures to ensure that other market participants cannot trade upon the basis of exposed confidential trade data. A third party with improper access could trade against a firm or use the data to reverse-engineer and clone trading strategies. Thus, robust systems and controls at Data Repositories and Regulated Entities are necessary to protect investors and promote market integrity.

MFA believes that Data Repositories and Regulated Entities must provide appropriate safeguards to ensure the confidentiality of sensitive and proprietary information, particularly under circumstances in which regulations require market participants to furnish such data to Data Repositories, self-regulatory organizations, designated contract markets, designated clearing organizations or clearinghouses, among others. Accordingly, we respectfully urge the Commissions to require and confirm that Data Repositories and other regulated entities maintain robust policies, practices and controls to protect the confidentiality of sensitive and proprietary information, including the identity of traders and the nature of their trading activities.

Recommendation: MFA recommends that the Commissions require and confirm that Data Repositories and other regulated entities maintain robust policies, practices and controls to protect the confidentiality of sensitive and proprietary information, including the identity of traders and the nature of their trading activities.

IV. Conclusion & Recommendations

MFA has consistently supported reasonable reporting requirements to ensure that regulators have meaningful data upon which to make policy decisions. Strong confidentiality

[46] CFTC Final Rule on "Swap Data Repositories: Registration Standards, Duties and Core Principles", 76 Fed. Reg. 54538 (Sept. 1, 2011), available at: http://www.gpo.gov/fdsys/pkg/FR-2011-09-01/pdf/2011-20817.pdf.

protections help foster an atmosphere of trust to ensure that reporting entities are as forthcoming as possible while safeguarding investors and promoting market integrity. Accordingly, we make a number of recommendations:

Recommendation 1: MFA recommends that the Commissions review and harmonize policies and controls concerning the treatment of sensitive and proprietary information.

Recommendation 2: MFA recommends that Regulators review the robustness of their policies, practices and controls relating to their use and treatment of sensitive and proprietary information and adopt such enhancements as are necessary.

Recommendation 3: MFA recommends that Regulators heighten staff sensitivity and awareness on the handling of non-public, sensitive and proprietary information through annual trainings and certifications, and regular reminders.

Recommendation 4: MFA recommends that FSOC Member Agencies implement a uniform system for sharing and protecting non-public information; such uniform system should include detailed controls and procedures around the access, documentation and use of non-public information, and be tailored appropriately for the level of sensitivity of the information.

Recommendation 5: MFA recommends that the Commissions require and confirm that Data Repositories and other regulated entities maintain robust policies, practices and controls to protect the confidentiality of sensitive and proprietary information, including the identity of traders and the nature of their trading activities.

Appendix A

Section 8(a) of the CEA provides:

For the efficient execution of the provisions of [the CEA], and in order to provide information for the use of Congress, the [CFTC] may make such investigations as it deems necessary to ascertain the facts regarding the operations of boards of trade and other persons subject to the provisions of this Act. The [CFTC] may publish from time to time the results of any such investigation and such general statistical information gathered therefrom as it deems of interest to the public: *Provided*, That except as otherwise specifically authorized in this Act, ***the [CFTC] may not publish data and information that would separately disclose the business transactions or market positions of any person and trade secrets or names of customers*** . . . **(emphasis added)**.[47]

Section 24(b) of the Exchange Act provides:

(b) It shall be unlawful for any member, officer, or employee of the Commission to disclose to any person other than a member, officer, or employee of the Commission, or to use for personal benefit, any information contained in any application, statement, report, contract, correspondence, notice, or other document filed with or otherwise obtained by the Commission (1) in contravention of the rules and regulations of the Commission under section 552 of Title 5, United States Code, or (2) in circumstances where the Commission has determined pursuant to such rules to accord confidential treatment to such information.

Section 204(b) of the Advisers Act provides:

(8) COMMISSION CONFIDENTIALITY OF REPORTS.—Notwithstanding any other provision of law, the Commission may not be compelled to disclose any report or information contained therein required to be filed with the Commission under this subsection, except that nothing in this subsection authorizes the Commission—
(A) to withhold information from Congress, upon an agreement of confidentiality; or
(B) prevent the Commission from complying with—
(i) a request for information from any other Federal department or agency or any self-regulatory organization requesting the report or information for purposes within the scope of its jurisdiction; or
(ii) an order of a court of the United States in an action brought by the United States or the Commission.
(9) OTHER RECIPIENTS CONFIDENTIALITY.—Any department, agency, or self-regulatory organization that receives reports or information from the Commission under this subsection shall maintain the confidentiality of such reports, documents, records, and information in a manner consistent with the level of confidentiality established for the Commission under paragraph (8).
(10) PUBLIC INFORMATION EXCEPTION.—

47

(A) IN GENERAL.—The Commission, the Council, and any other department, agency, or self-regulatory organization that receives information, reports, documents, records, or information from the Commission under this subsection, shall be exempt from the provisions of section 552 of title 5, United States Code, with respect to any such report, document, record, or information. Any proprietary information of an investment adviser ascertained by the Commission from any report required to be filed with the Commission pursuant to this subsection shall be subject to the same limitations on public disclosure as any facts ascertained during an examination, as provided by section 210(b) of this title.

(B) PROPRIETARY INFORMATION.—For purposes of this paragraph, proprietary information includes sensitive, non-public information regarding—

(i) the investment or trading strategies of the investment adviser;

(ii) analytical or research methodologies;

(iii) trading data;

(iv) computer hardware or software containing intellectual property; and

(v) any additional information that the Commission determines to be proprietary.

Appendix B

The National Institute of Standards and Technology provides that an effective information security program should include:

- Periodic assessments of risk, including the magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the organization.
- Policies and procedures that are based on risk assessments, cost-effectively reduce information security risks to an acceptable level, and ensure that information security is addressed throughout the life cycle of each organizational information system.
- Subordinate plans for providing adequate information security for networks, facilities, information systems, or groups of information systems, as appropriate.
- Security awareness training to inform personnel (including contractors and other users of information systems that support the operations and assets of the organization) of the information security risks associated with their activities and their responsibilities in complying with organizational policies and procedures designed to reduce these risks.
- Periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually.
- A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the information security policies, procedures, and practices of the organization.
- Procedures for detecting, reporting, and responding to security incidents
- Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the organization.

More information on NIST information security standards is available at: http://csrc.nist.gov/groups/SMA/fisma/overview.html.