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

May 16, 2008

VIA ELECTRONIC MAIL:
rule-comments@sec.gov

Attention: Nancy M. Morris, Secretary
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549

Re: Part 248 – Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information; File No. S7-06-08

Ladies and Gentlemen:

Managed Funds Association ("MFA")[1] appreciates the opportunity to comment on the U.S. Securities and Exchange Commission's ("SEC" or the "Commission") proposed amendments to Regulation S-P (the "Proposed Rule"), which implements certain provisions of the Gramm-Leach-Bliley Act ("GLBA") and the Fair Credit Reporting Act ("FCRA") for entities regulated by the Commission.[2]

MFA Comments and Recommendations on the Proposals in the Release

MFA supports the Commission's efforts to amend Regulation S-P to help prevent and address data security breaches in the securities industry in order to better protect investor information. We are concerned, however, that certain proposed amendments do not appropriately achieve the GLBA's goal of protecting a customer's non-public personal information. Therefore, we believe a number of modifications to the proposals are necessary to better align the provisions with the intent of the GLBA. We respectfully submit our comments and recommendations below.

I. Comprehensive Information Security Program

The Proposed Rule requires every investment adviser, broker-dealer, investment company, and transfer agent registered with the Commission (a "Registrant") to develop, implement, and maintain a comprehensive "information security program." Such a program

[1] MFA is the voice of the global alternative investment industry. Its members include professionals in hedge funds, funds of funds and managed futures funds. Established in 1991, MFA is the primary source of information for policy makers and the media and the leading advocate for sound business practices and industry growth. MFA members represent the vast majority of the largest hedge fund groups in the world who manage a substantial portion of the approximately $2 trillion invested in absolute return strategies. MFA is headquartered in Washington, D.C., with an office in New York.

[2] SEC Release No. 34-57427 (Mar. 13, 2008), 73 FR 13692 (the "Release").

would be beneficial to investors as it would protect and preserve the confidentiality and integrity of customer information. The Proposed Rule is consistent with the information security program standards developed by the Federal Trade Commission ("FTC"), and the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation and the Office of Thrift Supervision (collectively, the "Banking Agencies"), as required by the GLBA.[3] We support the Commission's efforts to achieve regulatory consistency and encourage the Commission to continue its coordination and consultation with the FTC and the Banking Agencies in formulating rules for Registrants under the GLBA.

A. Coordinator of the Information Security Program

The Proposed Rule requires a Registrant to designate in writing a specific employee or employees to coordinate the Registrant's information security program. MFA supports the concept of having an employee or employees responsible for coordinating a Registrant's information security program, but believes that the requirement to designate an employee in writing lacks flexibility as it ties the coordinator role to a specific individual. The Proposed Rule would require a Registrant to revise its policies and procedures each time it appointed a new employee coordinator or accounted for the departure of a former coordinator. As an alternative approach, we recommend that the Commission require a Registrant to designate in writing the responsibility of coordinating its information security program to a particular job title or function. This approach would be consistent with the approach taken by the Banking Agencies, and would address the goal of requiring a Registrant to formally designate a person or persons to coordinate the information security program.

B. Definition of Substantial Harm or Inconvenience

The Proposed Rule requires that a Registrant's information security program be reasonably designed to protect against unauthorized access to or use of personal information that could result in substantial harm or inconvenience. The proposed definition of the term "substantial harm or inconvenience" is "personal injury, or more than trivial financial loss, expenditure of effort or loss of time." We agree that any information security program should protect against substantial harm or inconvenience, but are concerned that the Commission has defined the term in a manner which sets the bar for loss or inconvenience too low as any financial loss, expenditure of time or loss of time that is scarcely "more than trivial" would be considered "substantial." Moreover, any degree of personal injury would also be considered "substantial" according to the definition. We recommend that the Commission revise the definition to reflect a

[3] *See* FTC, Standards for Safeguarding Customer Information, 67 FR 36484 (May 23, 2002); Banking Agencies, Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Recission of Year 2000 Standards for Safety and Soundness, 66 FR 8616 (Feb. 1, 2001). Pursuant to the GLBA, Regulation S-P must be consistent with and comparable to the financial privacy rules adopted by other federal financial regulators. *See* SEC, Privacy of Consumer Financial Information (Regulation S-P), 65 FR 40334 (June 29, 2000); FTC, Privacy of Consumer Financial Information, 65 FR 33646 (May 24, 2000); Banking Agencies, Privacy of Consumer Financial Information, 65 FR 35162 (June 1, 2000); and National Credit Union Administration, Privacy of Consumer Financial Information; Requirements for Insurance, 65 FR 31722 (May 18, 2000). *See also* 15 U.S.C. 6804(a)(2) (directing federal financial regulators to consult and coordinate to assure, to the extent possible, that each agency's regulations are consistent and comparable with the regulations prescribed by the other agencies).

higher standard for personal injury and loss and provide clarification of the actions that meet the standard.

II. Data Security Breach Response

The Proposed Rule requires that information security programs include written policies and procedures for responding to unauthorized access to or use of personal information. These policies and procedures would require a Registrant to provide notice, as soon as possible, to (1) affected individuals if an unauthorized person has obtained access to or used sensitive personal information and misuse of the information has occurred or is reasonably possible; and (2) the Commission (or for broker-dealers, their designated examining authority) when there is a significant risk that the individual identified with the information breach might suffer substantial harm or inconvenience, or when an unauthorized person has intentionally obtained access to or used sensitive personal information.

A. Notification to Individuals

MFA agrees with the Commission's emphasis on the importance of informing affected individuals regarding the misuse of sensitive personal information or the fact that such misuse is reasonably possible. It is equally important, however, that affected individuals actually receive notices that address real risks and review the notices upon receipt. As written, the Proposed Rule requires a Registrant to provide notice to an affected individual whenever misuse of information is "reasonably possible." We are concerned that the "reasonably possible" standard may result in a Registrant sending notices to customers each time it is reasonably possible, no matter how remote the chance, for the misuse of information. This approach seems likely to result in a significant number of notices being sent to customers, which would diminish the usefulness of the notification tool as individuals would possibly become desensitized to these notices over time and disregard them. As a result, affected individuals may overlook incidents that pose a real risk of misuse of their sensitive personal information. In addition, this approach would be costly and unduly burdensome to a Registrant.

The GLBA directed the Commission to adopt standards that would protect customer records and information against any unauthorized access to or use of those records or information, which could result in substantial harm or inconvenience to any customer. As a result, we urge the Commission to consider revising its provisions relating to the notification of individuals of the unauthorized access or use of sensitive personal information to require notification only if there is a risk of substantial harm or inconvenience to the affected individual. We believe that this approach is consistent with the intent of the GLBA and would provide customers of a Registrant with more useful and relevant information, which would allow them to better assess whether they need to take precautionary measures.

B. Notification to the Commission

MFA fully supports notifying the Commission when there is a significant risk that the individual identified with the information breach might suffer substantial harm or inconvenience. The Release indicates "the proposed notice requirement is intended to avoid notice to the Commission in every case of unauthorized access, and to focus scrutiny on information security

breaches that present a greater potential likelihood for harm."[4] To ensure that this objective is met, we recommend that the Commission provide guidance to assist Registrants in determining when there is a significant risk that the affected individual might suffer substantial harm or inconvenience that will trigger the notice to the Commission.

The Proposed Rule also requires notice to the Commission when an unauthorized person has intentionally obtained access to or used sensitive information. This proposal is overbroad and does not approximate the intent of the Commission to focus on breaches that have a greater likelihood for harm. For example, under this requirement a Registrant would have to notify the Commission of each instance where a customer's spouse, who was not listed on the account, accessed the account. In this instance, requiring notification where there is no risk of substantial harm or inconvenience would result in over-notification to the Commission and make it difficult for the Commission to discern breaches which pose a real risk of identity theft. Moreover, over-notification poses a burden on both the Registrant's and the SEC's resources. We recommend that the Commission limit Commission notifications to instances where there is significant risk that an individual might suffer substantial harm or inconvenience.

C. Form SP-30

The Commission proposes that Registrants use proposed Form SP-30 (the "Proposed Form") to provide notice to the Commission or the appropriate designated examining authority. The Proposed Rule requires the filing of the Proposed Form as soon as possible after the Registrant becomes aware of a significant breach. The Proposed Form raises a number of concerns. First, the Proposed Form requires a level of detail and information, such as net customer losses, that may be unavailable upon becoming aware of a breach, which would make filing the Proposed Form in the time frame required very difficult or would result in the filing of an incomplete or inaccurate document requiring continuous update as additional information becomes available. Second, the information gathering process necessary for the completion of the Proposed Form could detract time and resources from and may hinder the Registrant's investigation into the breach. We believe requiring the Proposed Form to be filed with the Commission immediately upon discovery of a significant breach would be premature, and not particularly helpful to the Commission.

Alternatively, we propose that the Commission require a Registrant to file with the Commission the same notice provided to the customer who experienced the information breach to satisfy its reporting requirement to the Commission. A Registrant would file a notice describing the incident and the type of sensitive personal information that was the subject of the unauthorized access or use, as well as the actions taken by the Registrant to protect the individual's information from further unauthorized access or use. This information would highlight for the Commission the relevant facts necessary to evaluate whether any legal action against a would-be identity thief or other action is warranted under the circumstances.

We note that the Banking Agencies, in their Incident Response Guidance, also considered the use of a standardized notice for regulator notification. They ultimately rejected the use of a standardized form, however, because they did not want to burden financial institutions with a detailed process. Instead, financial institutions are required to contact their primary regulator as

[4] 73 FR 13692, 13698.

quickly as possible, by telephone, or in some other expeditious manner when the institution becomes aware of the breach.[5] As far as we're aware, this process has been effective for the Banking Agencies.

We recommend that the Commission allow a Registrant to satisfy its reporting obligation by sending to the Commission the same notification that the Registrant will send to individuals identified with an information breach.

III. Expansion of the Definition of Personal Information under the Safeguarding and Disposal Rules

The Commission proposes to expand the scope of the term "personal information" as defined under the GLBA safeguards requirements and the FCRA disposal rules. The Proposed Rule defines personal information to include any record containing either nonpublic personal information or consumer report information, as well as information identified with any consumer, or with any employee, investor, or security holder who is a natural person.[6] The GLBA and FCRA require the Commission to establish appropriate standards for Registrants to safeguard and dispose of *customer* records and information, not employee, investor or security holder records or information. We believe that defining personal information in this manner is outside the scope of the GLBA and the FCRA and, therefore, outside of the Commission's rulemaking authority. Moreover, this definition would not be consistent with or comparable to the definition used by the FTC and the Banking Agencies as mandated by the GLBA. Accordingly, we recommend that the Commission limit its definition of personal information to customer records or information.

In the Proposed Rule, the Commission requested comments on the expansion of the proposed definition of "personal information" to include information identified with non-natural persons such as corporate clients. The Release did not contain any discussion regarding the necessity of this protection for corporate entities. The GLBA and FCRA contemplate protecting natural persons only. We believe application of the GLBA and FCRA to non-natural persons would require Congressional action. Thus, the Commission would be exceeding its authority under these statutes if it sought to protect such persons through rulemaking.

IV. Exception for Limited Information Disclosure When Personnel Leave Their Firms

The Commission proposes to add a new exception from the notice and opt out provisions of Regulation S-P to permit limited disclosures of investor information when a registered representative of a broker-dealer or a supervised person of a registered investment adviser moves from one brokerage or registered investment advisory firm to another. We fully support this proposal as it promotes customer choice by making it easier for a customer to receive information regarding the departing individual's new employment and to choose where he or she wants to maintain a relationship after a representative or supervised person changes firms. Moreover, the proposal provides legal certainty and reduces potential incentives for improper disclosures.

The Commission also solicited comments on the extension of this exception to information use and sharing when moving from an SEC registered adviser to an unregistered

---

[5] *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 FR 15736, 15741 (Mar. 29, 2005).

[6] *See* Proposed Rule 248.30(d)(8).

adviser. We would encourage the Commission to create a similar exception in this instance for the same reasons cited above. We urge the Commission to discuss this exception with the FTC, which promulgates rules under the GLBA for unregistered advisers, and encourage the FTC to create a similar exception for unregistered advisers who move to another unregistered adviser or to an SEC registered adviser in accordance with the coordination requirement of the GLBA.

V. Compliance Period

The Release does not discuss the compliance or transition period for the Proposed Rule, if adopted. We are concerned that a number of the proposed amendments would require substantial changes to a Registrant's existing computer systems, recordkeeping and retention processes, particularly with regard to capturing the information required by the proposed definition of personal information under the safeguarding and disposal rules. Moreover, the preparation, risk evaluation, testing and implementation of written policies and procedures for an information security program, as contemplated by the Proposed Rule, will require ample time and a significant allocation of a Registrant's resources. Registrants must have sufficient time to implement any new requirements properly. In light of these considerations, we recommend that the final rules include a transition period of at least 18 months.

* * *

Conclusion

MFA appreciates this opportunity to comment on the proposed amendments to Regulation S-P. We would be pleased to meet with the Commission or its Staff to discuss our comments further. Please feel free to call me at (202) 367-1140.

Respectfully submitted,

Richard H. Baker
President and Chief Executive Officer

cc: The Hon. Christopher Cox, Chairman
The Hon. Paul S. Atkins, Commissioner
The Hon. Kathleen L. Casey, Commissioner
Andrew Donohue, Director
Division of Investment Management
Erik Sirri, Director
Division of Trading and Markets