SIFMA
Securities Industry and Financial Markets Association

May 12, 2008

Via Electronic Mail

Nancy M. Morris
Secretary
Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549-1090

Re: File Number S7-06-08; Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information

Ladies and Gentlemen:

The Securities Industry and Financial Markets Association ("SIFMA")[1] appreciates the opportunity to comment on the proposed amendments of the Securities and Exchange Commission (the "Commission") to Regulation S-P, Privacy of Consumer Financial Information and Safeguarding Personal Information.[2] The securities industry has long recognized the importance of protecting customers' nonpublic personal information and strongly supports the safeguarding provisions of the Gramm-Leach-Bliley Act ("GLBA"). Our member firms have worked diligently to effectively ensure the security and confidentiality of customer information in accordance with the GLBA and Regulation S-P.

We commend the Commission on its efforts to review the standards currently reflected in Regulation S-P relating to safeguarding customer records and information and standards for responding to data security breaches. We believe that the Commission's proposed amendments are a clear step in the right direction for achieving the objectives set out by Congress in § 501 of the GLBA.

Our recommendations include the following: 1) the revisions to Regulation S-P should be harmonized with the Federal Banking Agencies' Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice; 2) a firm should be required to implement an information security program that is appropriate to its size and business; 3) the rule should not be expanded to cover employees, investors and security holders which are all beyond the scope of GLBA; 4) firms should only be required to notify the government of a breach if more than 1,000 customers are affected, and the method of notification should be flexible; 5) the proposed exception permitting departing registered representatives to take their customer contact information to their new firm should be clarified; and 6) the rule should provide firms with an 18 month implementation period. We also make several recommendations to clarify other provisions of the proposal.

[1] SIFMA brings together the shared interests of more than 650 securities firms, banks and asset managers. SIFMA's mission is to promote policies and practices that work to expand and perfect markets, foster the development of new products and services and create efficiencies for member firms, while preserving and enhancing the public's trust and confidence in the markets and the industry. SIFMA works to represent its members' interests locally and globally. It has offices in New York, Washington D.C., and London and its associated firm, the Asia Securities Industry and Financial Markets Association, is based in Hong Kong.

[2] 73 *Fed. Reg.* 13692 (March 13, 2008).

General Overview

SIFMA believes that the Commission should carefully assess the effects of the proposed amendments and should not impose unnecessary additional burdens on securities firms. Because of the extensive affiliations between securities firms and banking organizations, SIFMA believes that it is important for the Commission to harmonize Regulation S-P with the guidance provided by the Federal banking agencies.[3] Consistency with the guidance of the Federal banking agencies is of particular importance to securities firms affiliated with banking organizations which have implemented policies and procedures and developed systems, applications and processes in accordance with standards of the banking agencies. As a result of such consistency, securities firms will be better positioned to address compliance with the uniform standards adopted by all of the Federal agencies. Applying standards to securities firms that are inconsistent with those applicable to banking organizations would prove unduly burdensome for some securities firms. Accordingly, SIFMA supports the proposed amendments to the extent that they are consistent with the guidance of the federal banking agencies and take into account the unique differences inherent in the securities industry.

SIFMA also supports the standard that an information security program should be appropriate to the firm's size and complexity, nature and scope of activities and the sensitivity of personal information at issue. In this regard, SIFMA believes that the final rule should expressly indicate that in developing their programs, firms may employ a risk-based approach, taking into account cost-benefit analyses. The Commission should also confirm that a diversified financial institution complex which includes a securities firm may adopt a single information security program across all companies within the financial services organization. This would enable a firm to take a consistent approach and harmonize information security programs across the entire organization

The Commission asks whether the rule's requirements should specify factors such as those identified in the banking agencies' guidance regarding authentication in an Internet environment, or include policies and procedures such as those in the banking agencies' "red flags" requirements. SIFMA believes that it is unnecessary for the Commission to adopt these additional requirements at this time. Given the rapidly evolving nature of how transactions are conducted over the Internet, and the fact that financial institutions will be implementing the new red flags requirements under the banking agencies' guidance over the next several months, SIFMA suggests that the Commission defer any action in this area. Rather, the Commission could monitor the effects of the banking agencies' guidance over the next year or so before considering adopting these additional requirements.

Scope of Coverage

The proposed revision covers consumers, employees, investors and security holders who are natural persons. Section 501 of the GLBA provides that financial institutions have an affirmative and continuing obligation to protect the security and confidentiality of their customers' nonpublic personal information.[4] In furtherance of this objective, § 501(b) authorizes the Commission and other Federal agencies to establish appropriate standards for financial institutions to insure the security and

[3] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. 70 *Fed. Reg.* 15736.
[4] 15 U.S.C. § 6801(a).

confidentiality of customer information. There is nothing in § 501 of the GLBA that applies the standards set forth therein to employee information. Moreover, the guidance of the banking agencies and guidance of the Federal Trade Commission do not extend to employee information. SIFMA believes that in view of the specific language of § 501, and in order to be consistent with the requirements of the other Federal agencies, it is inappropriate to expand the scope of the proposed rule to cover employee information.

In addition, the Commission should revise the proposed rule to clarify that nonpublic personal and sensitive personal information of persons who are not customers, including investors and security holders who may not be customers, does not fall within the scope of coverage since § 501 only applies to information of individuals who are customers of the financial institution.

The Commission also asks whether the proposed definition of personal information should be expanded to include information identified with non-natural persons, such as corporate clients. SIFMA opposes such an expansion. Section 501 of the GLBA authorizes the agencies to establish appropriate standards relating to safeguarding customer information. The GLBA applies only to individuals who obtain financial services primarily for personal, family or household purposes and Regulation S-P defines the term "customer" as a consumer who has a customer relationship with the firm. 15 U.S.C. § 502(a) and Regulation S-P § 248.3(j). Accordingly, we see no legal basis for the Commission to expand the scope of coverage when it is clear that Congress intended to apply § 501 solely to nonpublic personal information concerning natural persons.

Not only do the above referenced proposals go beyond the GLBA statutory authority, but SIFMA believes that the GLBA focus on individual consumer and customer information is the correct approach. In addition, since the GLBA was adopted firms have developed all of their policies, procedures, systems, applications and processes based on the GLBA framework and defined terms. SIFMA strongly believes that expanding definitions or scope is not necessary or authorized, and to do so at this time would cause confusion and require extensive retooling of well-established systems and processes. SIFMA believes that the existing GLBA framework and definitions are sound, and additional requirements should build upon such existing framework and definitions.

Use of Examples

SIFMA believes that the examples of acceptable practices set forth in the *Federal Register* preamble to the proposed rule are very helpful to firms because they present real practical situations that firms may encounter. In order to maximize their benefit, SIFMA requests that the Commission incorporate these examples into the final rule rather than simply leaving them in the *Federal Register* preamble. However, the Commission should also indicate that the examples are illustrative of acceptable practices and are not prescriptive.

Designation of Responsible Employee

The Commission asks whether institutions should be required to designate an employee or employees to coordinate the information security program by name or should the designations be by position or office. SIFMA firmly believes that institutions should have the flexibility to choose either option. Some firms may wish to name a specific employee to coordinate the information security program

while others may wish to indicate a particular position, office or function. Accordingly, SIFMA requests that the Commission provide institutions with the option to decide how to designate the appropriate person or area with the responsibility to coordinate the firm's information security program. In addition, SIFMA requests that the Commission also permit a securities firm that is part of a diversified financial services complex to designate an employee of an affiliate or a position at an affiliate as the person or area responsible for coordinating the company's information security program. Such flexibility assists in ensuring that the policies of such firms are consistent and coordinated throughout the firm as a whole.

Substantial Harm or Inconvenience

The Commission proposes that a firm'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. It is proposed that the term "substantial harm or inconvenience" be defined as "personal injury, or more than trivial financial loss, expenditure of effort or loss of time." SIFMA believes that this standard is incorrect because it treats any financial loss that is slightly above "trivial" as "substantial." Moreover, it regards any personal injury, no matter how insignificant as "substantial." SIFMA recommends that the standard be established at a level that is consistent with the usual meaning of the term "substantial." Accordingly, SIFMA requests that the term "substantial harm or inconvenience" be defined as "significant personal injury, financial loss, expenditure of effort or loss of time." Such a definition is more consistent with the customary use of the term than is the proposed definition. In addition, the definition should not include activities such as harassment and intimidation, which firms are not in a position to assess.

SIFMA agrees with the Commission's view that a change to an account number or password is not "substantial harm," nor is unintentional delivery of an account statement to an incorrect address if the information was unlikely to be misused. The Commission's example that accidental access by an employee to a customer's records would not constitute substantial harm or inconvenience if there is no significant risk of misuse should be expanded to include employees of affiliates and service providers of the firm, as well as "good faith acquisition" of personal information by such parties. In this context, SIFMA requests that the Commission consider expressly including these as well as additional examples in the final rule.

Notice and Form SP-30

In its *Federal Register* preamble, the Commission indicates that 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.[5] However, despite this language, the proposed rule requires broker-dealers to provide written notice to their designated examining authority on Form SP-30 as soon as possible after becoming aware of an incident of unauthorized access to, or use of, personal information in which (1) there is a significant risk of substantial harm or inconvenience to the individual, or (2) an unauthorized person has intentionally obtained access to or used sensitive personal information (emphasis added). SIFMA believes that notice to the designated examining authority should be required only if there is a significant risk of substantial harm or inconvenience to the individual. In light of the Commission's express desire to avoid notice to

[5] 73 *Fed. Reg.* at 13698.

the Commission in every case of unauthorized access, and to focus scrutiny on information security breaches that present a greater potential likelihood for harm, we see no reason why notice to the Commission or the firm's designated examining authority should be required if an unauthorized person has obtained access to or used sensitive personal information and there is no significant risk of substantial harm or inconvenience to the individual. Such notices will serve no useful purpose and are an unnecessary administrative burden. Moreover, the proposed rule is likely to require over-notification, particularly in instances in which a firm may not be required to notify affected customers. For example, there may arise situations where a firm determines that the likelihood of misuse of the information has not occurred nor is reasonably possible. However, proposed § 248.30(a)(v)(B) could require written notice to the designated examining authority or to the Commission. Accordingly, SIFMA recommends that notice to the firm's designated examining authority or to the Commission be required only if there is a significant risk that a customer might suffer substantial harm or inconvenience. Finally, we believe that a notice to the designated examining authority should be required only if the firm estimates that 1000 or more individuals are or will be affected by the incident.[6] Incidents that affect less than 1000 individuals are generally not a major incident and notice would be unnecessary burden on firms and the government.

SIFMA also believes that the proposed Form SP-30 should not be adopted. First, the Federal banking agencies do not require financial institutions subject to their jurisdiction to use a specific form, and this process has worked well. In addition, the added burden and unnecessary specificity of the Form SP-30 would require significant additional resources to comply with the new reporting requirements. The proposed form unrealistically presumes accurate and complete information is available at the early stages of a potential breach and requires detailed reporting that is likely not available or not accurate at that early stage. Because the proposed rule requires the submission of Form SP-30 as soon as possible after becoming aware of an incident of unauthorized access to or use of personal information, there is little likelihood that a firm would have all or substantially all of the information requested by the form. Moreover, information submitted on the initial forms will undoubtedly change and would have to be amended as additional information is obtained. Accordingly, as facts regarding the situation are determined, firms would be required to submit numerous additional forms to supplement the original filing, taking resources away from the internal effort to assess, respond to, and limit impact of the breach. This will undoubtedly lead to confusion resulting from the need to submit seemingly contradictory information.

SIFMA believes that a better approach would be the method adopted by the Federal banking agencies, which does not specify the details or method of the report, and which permits the institution to contact the regulators by various means, including by phone. The Commission's rule could simply include examples of the types of information that firms may wish to consider including in the report. For example, the name of the firm, dates of the incident and the filing, a brief description of the incident, a preliminary estimate of the number of persons affected and whom to contact for more information would appear to be more than sufficient information to meet the Commission's needs. Instead, the Commission's proposal would require a complicated filing that will place firms in a difficult position by requiring detailed information that may not yet be final. This could lead to repeated updates to the Form SP-30 submissions. The rule should therefore require only a short notice to the regulator, as is required by the banking agencies. If the Commission or staff of the designated examining authority regards it as

[6] *See e.g.*, Hawaii's breach notification statute which requires notice if more than 1,000 individuals are affected by a security breach. HRS § 487N-2(f).

appropriate to follow-up with a firm, it may seek more information as it does with other types of confidential inquiries.

The Commission indicates that it is concerned in particular with fraud relating to account takeovers, including the use of accounts as part of "pump and dump" schemes, as well as "phishing" attacks. SIFMA believes that incidents involving these kinds of fraudulent activities typically do not involve information security breaches at firms. Rather, such incidents typically are the result of fraud perpetrated on the customer that enables the fraudster to gain access to the customer's account by tricking the customer into revealing his or her password and user ID. These schemes are not firm information security breaches and should not be subject to the proposed security breach notice provisions of Regulation S-P. Rather, SIFMA believes that the Commission should develop a separate initiative to address these incidents as fraudulent transactions, and we understand that the Commission staff and the industry have been coordinating on these issues.[7] Further, we believe that if a firm has filed a Suspicious Activity Report in connection with the incident, the firm should not be required to file a separate notice with its designated examining authority.

Finally, SIFMA believes that the information reported to the Commission in connection with a data breach is the type of information that should not be available to the public. The information requested generally relates to information that is regarded by firms as confidential business information, the public disclosure of which would likely be competitively harmful. The information reported by firms will also be sensitive information potentially helpful to breach offenders. Rather than requiring firms to request confidential treatment of the information every time it is submitted, SIFMA believes that the Commission should indicate that filings made with the Commission by firms in accordance with Regulation S-P will be accorded confidential treatment under the Freedom of Information Act and the Commission's rules regarding public availability of information. If any of this information is made public, it should be released only in an aggregated and summary format.

With respect to notice to customers, the Commission should clarify that the proposed rule does not require institutions to maintain a written record of each determination that misuse of information has not occurred or is not reasonably possible. Such a requirement to create documentation of each determination where misuse was deemed unlikely is impractical and burdensome. For example, it could mean that every time an email is sent to an incorrect address, specific documentation concerning a determination that misuse is unlikely would be required. Similarly, the Commission should clarify that the proposed rule does not require a separate specific written record of the determination to make such notification, but that the written notification itself is sufficient.

Definition of Sensitive Information

SIFMA is very concerned that the Commission's proposed definition of "sensitive personal information" as set forth in the proposed rule is overly broad and well beyond the definition adopted by the Federal banking agencies of the term "sensitive customer information."[8] It is proposed that "sensitive personal information" also means "personal information." "Personal information" is defined as "any

[7] In addition, SIFMA believes that because pump and dump schemes demonstrate the vulnerabilities of the Internet more coordination with ISPs, law enforcement and other stake holders needs to occur in order to deter such fraudulent activities.
[8] *See e.g.,* 70 *Fed. Reg.* at 15752.

record containing consumer report information, or nonpublic personal information as defined in § 248.3(t)." As a result, virtually all information maintained by a firm will be regarded as "sensitive personal information." Accordingly, a firm will be required to notify customers when it believes misuse of essentially any information is reasonably possible. This is a significant departure from the standards used by the other Federal agencies, which define "sensitive personal information" far more reasonably. We suggest that the Commission define sensitive personal information in exactly the same way the other agencies have defined "sensitive customer information" and most state laws have defined it, which is substantially similar to the definition proposed in the latter portion of § 248.30(d)(10).

In this regard, the Commission's proposed definition of sensitive personal information also includes a person's Social Security Number ("SSN"), as well as other information such as a mother's maiden name. This too differs from the other agencies' definition which regards an SSN as sensitive customer information only if used in combination with the person's name, address or telephone number. We do not understand how a person's SSN alone can be regarded as "sensitive personal information" unless it is obtained in combination with other information that would permit access to a customer's account. Moreover, a mother's maiden name should not be regarded as sensitive personal information unless the name is used as a password for access to a person's account. In the interests of consistency, SIFMA believes that it would be preferable and less confusing if the Commission adopted the definition of "sensitive customer information" adopted by the banking agencies.

In addition, SIFMA believes that any information that is encrypted should not be regarded as sensitive personal information unless there is reason to believe that the encryption key has been compromised. While this specific exception is not in the text of the banking agency guidance, it is consistent with how such requirements are applied. Additionally, this approach is consistent with numerous state laws that regard information as sensitive personal information only if it is unencrypted.[9] SIFMA believes that encrypted information should not be regarded as sensitive personal information because the risk of misuse of such information is virtually non-existent. At a minimum, the Commission should affirmatively acknowledge that encryption is a factor that firms may take into account in determining whether an incident will result in substantial harm, inconvenience, or misuse.

Service Providers

The proposed rule defines a service provider as any entity that receives, maintains, processes or otherwise is permitted access to personal information through its provision of services to the firm. Accordingly, the proposed rule treats a firm's affiliate that provides services to the firm as a service provider. The proposed rule further provides that a firm's information security program must require the firm to oversee service providers and require them by contract to implement and maintain appropriate safeguards. SIFMA believes that it is inappropriate to treat affiliates that provide services to an affiliated firm as service providers under § 248.30(d)(11) for purposes of § 248.30. Many organizations are structured in a manner that makes it administratively beneficial for firms to obtain services from affiliates. These services often are provided by affiliates in a manner established by the organization's policies without the need for formal contracts because the affiliates are typically subject to company-wide policies and standards relating to safeguarding personal information. Moreover, the data security policies

[9] *See, e.g.*, California Information Practices Act of 1977, California Civil Code §1798.29(e).

of affiliates are typically subject to oversight by organizational component that monitors company compliance. To require that affiliate service provider arrangements be subject to oversight by each firm in the same organization it provides services to, and enter into formal contractual undertakings misperceives the nature of how companies interact with affiliates. Given the nature of these affiliate arrangements, SIFMA sees no purpose to be served by requiring a firm to exercise oversight of its affiliates and requiring it to enter into contracts with its affiliates to implement and maintain safeguards. We believe that support for this position can be found in another section of Regulation S-P, in which the Commission adopted an approach that recognizes the unique relationship between affiliates. Section 248.13(a)(1) establishes an exception from the GLBA opt-out requirements for information disclosures to affiliates that provide services to the firm. This exception provides implicit acknowledgement that there is little reason to treat affiliates as service providers.

SIFMA supports the position that firms may use third-party reports, such as a review of a service provider's SAS-70 or SysTrust reports, in order to assess the adequacy of service provider information safeguards. The Commission should also indicate that other methods for evaluating service provider information safeguards are acceptable as long as they are reasonable and based on the scope of services provided. Other methods could include, for example, a review of the service provider's audit report or other risk assessment if appropriate under the circumstances. In this regard, SIFMA believes that if the service provider is an entity subject to the GLBA, the Commission should permit firms to take the fact that the institution is subject to § 501's safeguards into account in their initial due diligence and in their continuing monitoring of service providers.

In addition, SIFMA believes that the Commission should clarify that the requirement for a written contract can be satisfied by incorporating the requirement in a clearing agreement which an introducing broker or other firm may enter into with its clearing firm.

Disposal of Personal Information

The proposed rule expands the current Commission rule regarding disposal of personal information by requiring firms to document in writing their proper disposal of personal information. This could suggest that a written record is required every time a firm disposes of any personal information, which would be a significant and unnecessary burden on firms. Firms should not be required to document every disposal of documents containing personal information. The Commission should simply require that firms have appropriate disposal policies and procedures and confirm that such disposal policies and procedures are being complied with by the firm. SIFMA also suggests that the disposal rule expressly indicate that firm employees are not personally liable in the event customer information is not properly disposed of.

The Commission asks whether the proposed periods of time for preserving records are appropriate. We think that firms that are part of diversified companies and subject to different record retention requirements should have the flexibility to apply one record retention period across affiliates as long as it satisfies the minimum required by each regulator.

Exception to GLBA for Departing Representatives

SIFMA appreciates the SEC's efforts to draft the exception for departing representatives and clarify what information departing representatives may take under Regulation S-P without their firms providing a notice and opt-out to the affected customers. This has been an issue that has not been entirely clear since Regulation S-P was promulgated.

Our firms have reviewed the proposed exception and approach this from different perspectives given the diverse business models represented in our membership – *e.g.*, full service firms, small or regional retail based firms, online firms, independent firms, discount firms, clearing firms and institutional firms. SIFMA firms have divergent views and policies regarding whether departing brokers should be permitted to take customer information with them.

Our comments are therefore directed at making the exception, if adopted, more workable. Accordingly, we believe that the rule needs to be clear that the exception simply provides an exception for the limited customer contact information that is identified in the proposed rule from the notice and opt-out requirements of Regulation S-P, and that the Commission does not require any particular practice or policy. For this reason, we recommend that the text of the rule provide that representatives are subject to their firm's policies and firms may, through their own policies, procedures or agreements, consistent with Regulation S-P, prohibit or permit representatives from taking any customer information, including the limited information provided by the exception. Moreover, firms should also be required to adopt written policies and procedures to implement the exception as well as identify the category of representatives to whom the policies apply. Therefore, we recommend that the first paragraph of the rule text, § 248.15(a)(8), be revised as follows (changes and additions underlined):

> To a broker, dealer, or investment adviser registered with the Commission, <u>provided that your policies and procedures expressly allow the transfer of limited customer contact and account information consistent with §248.15(a)(8)(i) of this exception,</u> in order to allow one of your representatives who leaves to become the representative of another broker, dealer, or investment adviser to <u>contact</u> customers <u>to the extent permitted by that policy, provided:</u>

In addition, the use of the word "including" in proposed §248.15(a)(8)(i) will likely be interpreted as permitting the disclosure of other information. Therefore, the word "including" in that provision should be deleted.

SIFMA also requests that the Commission clarify that information that a departing representative is permitted to take remains subject to the safekeeping policies of the firm while the information is in transit, that the departing employee is obligated to comply with such policies until the information is received by the employee's new firm, and that the new firm be subject to Regulation S-P.

In addition, SIFMA believes that the language "a general description of the type of account and products held by the customer" is too vague and overly broad. The exception provides that no notice or opt-out is required if the information a departing representative takes is limited to a customer's name, a general description of the type of account and products held by the customer and the customer's contact

information. Unlike language in the exception relating to name, address, telephone number and e-mail address, the language regarding types of account and product information does not precisely provide clear guidance as to the permitted information within the exception. SIFMA believes that a better approach would be to use the term "account title" as a more accurate description of the types of information that come within the exception. The term "account title" is commonly understood to mean the information of a given account that is usually contained on client account statements, such as: Mr. John Doe and Mrs. Jane Doe JTWROS; Jane Doe C/F Susie Doe UGMA/TX; or John Doe – SEP IRA. This account title information is helpful, providing the broker with the opportunity to speak to the customer about the type of accounts the customer has and whether the customer would like to transfer some or all of them.

Finally, the proposal indicates the type of information that is not included within the scope of the exception. SIFMA believes that it is neither desirable nor necessary for the rule to indicate what information is not included within the scope of the exception.

Cost Estimates

The Commission estimates that the initial cost of implementation for larger firms will be approximately $173,000 and $18,600 for smaller firms, and ongoing annual compliance costs are estimated to be $51,000 for larger firms and $10,700 for smaller firms. Based on rough estimates, we believe that the Commission's estimates vastly underestimate the costs for all firms to implement changes required by the proposal, and the annual compliance costs as well.

Effective Date

SIFMA is concerned that given the scope of the requirements of the rule, firms will not have sufficient time to implement the rule in an orderly fashion after it is adopted. The proposed rule does not indicate when it would become effective.[10] Our firms, especially smaller ones, advise that they will need 18 months after the rule is adopted to implement all of the necessary systems changes. This is because the proposal will require comprehensive changes to policies and procedures for both small and large firms to implement all of the elements of the newly required "information security program." Firms are especially concerned that the provision to require service providers by contract to maintain appropriate safeguards will be very time consuming because firms will have to review, negotiate and revise all contracts with service providers. Moreover, the term of many contracts with service providers extends for a year or more, and the service providers are under no legal obligation to re-open them to incorporate changes to Regulation S-P. Firms will also be required to establish procedures for responding to incidents of potential unauthorized access to or use of personal information. Firms that already have data breach procedures will have to review and revise such procedures to ensure compliance with Regulation S-P. Firms will also find it necessary to implement changes to their procedures to implement the safeguards and disposal rules to reflect the expanded definition of the information now subject to both rules. Compounding the need for additional time is the fact that many firms are already expending considerable

[10] The *Federal Register* preamble states, however, that if the rule is considered a "major" rule, its effectiveness will generally be delayed for 60 days. A rule is major if it has an annual effect on the economy of at least $100 million. Given even the Commission's implementation cost estimates, it is readily apparent that firms will incur expenses of at least $100 million to implement and comply with the final rule.

resources implementing the affiliate marketing rules and the identity theft red flags rules. In addition, all of this comes at a when the industry is still responding to the severe market disruptions of the past year.

Accordingly, SIFMA requests that the final rule provide firms with a compliance date 18 months after the effective date in order to implement the rule's requirements.

* * *

SIFMA greatly appreciates the opportunity to comment on the Commission's proposed amendments to Regulation S-P. If you wish to receive additional information related to these comments, please feel free to contact the undersigned.

Sincerely,

Alan E. Sorcher
Managing Director and
Associate General Counsel

cc: Catherine McGuire, Chief Counsel, SEC
Lourdes Gonzales, Assistant Chief Counsel, SEC
Brice Prince, Special Counsel, SEC