ABASA
ABA SECURITIES ASSOCIATION
An affiliate of the
AMERICAN BANKERS ASSOCIATION

1120 Connecticut Avenue, NW
Washington, DC 20036

202-663-5277
Fax: 202-828-4546
www.aba.com

World-Class Solutions, Leadership & Advocacy Since 1875

Sarah A. Miller
General Counsel
Phone: 202-663-5325
Fax: 202-828-5047
Email:
smiller@aba.com

Via Electronic Mail
May 22, 2008

Nancy M. Morris, Secretary
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Re: SEC Proposed Amendments to Regulation S-P
File Number S7-06-08
73 *Federal Register* 13692, March 4, 2008

Dear Ms. Morris:

The ABA Securities Association (ABASA) appreciates the opportunity to submit comments on the proposal of the Securities and Exchange Commission (the Commission) to amend its Regulation S-P, *Privacy of Consumer Financial Information and Safeguarding Personal Information*.

ABASA is a separately chartered affiliate of the American Bankers Association (ABA)[1] representing those holding company members of the ABA actively engaged in capital markets, investment banking and broker-dealer activities. Our members offer commercial and investment banking products and other financial services through separate legal entities. Many of their customers maintain both banking and securities relationships with a single holding company entity, and trust and expect that their sensitive customer information pertaining to all of their accounts is properly safeguarded. ABASA's members understand this critical obligation to safeguard customer data, and have in place longstanding information security programs pursuant to the regulations and guidance of the federal bank regulatory agencies.

At the outset, ABASA commends the Commission for its efforts to ensure that customer information is safeguarded, as well as for its stated goal of maintaining consistency with regulations and guidance issued by the federal bank regulatory agencies. ABASA certainly shares these goals. Nonetheless, we believe that a number of the proposed amendments would impose a level of reporting and recordkeeping detail that neither enhance customer information security nor permit essential consistency across financial holding companies. Many of the proposed

[1] The American Bankers Association brings together banks of all sizes and charters into one association. ABA works to enhance the competitiveness of the nation's banking industry and strengthen America's economy and communities. Its members – the majority of which are banks with less than $125 billion in assets – represent over 95 percent of the industry's $12.7 trillion in assets and employ over 2 million men and women.

amendments are unnecessarily inconsistent with existing bank regulatory guidance, and several, we respectfully submit, are outside the scope of the authority conferred upon the Commission under Title V of the Gramm-Leach-Bliley Act (GLBA).

As noted in the preamble to the proposal, since the Commission initially adopted Regulation S-P in 2001, the federal bank regulatory agencies, generally under the auspices of the Federal Financial Institution Examination Council (FFIEC), issued significant additional regulatory guidance to address the safeguarding of customer information in 2005 and 2006.[2] The FFIEC establishes uniform guidelines for depository institutions, bank holding companies and financial holding companies, and such interagency guidance and regulations provide an important level of consistency across the banking sector. Many integrated financial services companies have already implemented policies and procedures consistent with FFIEC guidance and regulations, including the requisite information systems and training programs necessary to implement such guidance and regulations. Moreover, in response to regulatory emphasis on enterprise-wide risk management, many firms have implemented the FFIEC requirements across the entire holding company. As a result, ABASA believes that it is essential that the Commission's regulations be as consistent as reasonably possible with the established safeguarding and data breach programs of the federal banking agencies so that integrated firms do not suffer significant costs to (1) change information systems that have only been in place for two or three years at the most, and (2) retrain employees as necessary. To warrant the imposition of such costs, we believe the Commission should be able to demonstrate that variations from the FFIEC guidance will result in a substantial increase in protection of consumer information. To do otherwise would require integrated financial services companies to expend limited corporate resources with little or no demonstrable benefit to protecting customer information.

Summary Recommendations

Specifically, our key recommendations are that:

- The definition of "substantial harm and inconvenience" be narrowed ;
- The scope of the persons and information covered by Regulation S-P remain consistent with Title V of GLBA;
- Security incident reporting Form SP-30 should not be adopted because it is unworkable from a practical perspective and raises significant and important issues concerning the possible release of a securities firm's confidential business information;
- The provision for departing registered representatives taking customer contact information to their new firm should be revised to make clear that notwithstanding the exception from the notice and opt-out requirements, firms have the sole authority to determine whether their policies prohibit or permit such movement of any or all customer contact information; and
- The effective date of the final rule should provide at least 18 months for implementation.

[2] See *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice,* 70 FR 15736 (March 29, 2005); and *Authentication in an Internet Banking Environment*, July 27, 2006, available at *www.ffiec.gov/pdf/authentication_guidance.pdf.*

Background

The Commission is proposing changes to Regulation S-P in response to the potential for identity theft and other misuse of personal financial information that have "spread throughout the business community, including the securities industry," and most particularly from the takeover of online brokerage accounts.[3] In addition, the Commission is concerned that "some firms do not regularly reevaluate and update their safeguarding programs to deal with these increasingly sophisticated methods of attack."[4] Accordingly, the proposal would amend Regulation S-P in four principal ways to:

- Require more specific standards under the safeguards rule, including standards that would apply to data security breach incidents;
- Amend the scope of the information covered by the safeguards and disposal rules and to broaden the types of institutions and persons covered by the rules;
- Require institutions subject to the safeguards and disposal rules to maintain written records of their policies and procedures and their compliance with those policies and procedures; and
- Propose a new exception from Regulation S-P's notice and opt-out requirements to allow departing representatives to take limited customer information when moving to a new firm.

Discussion

1. Revised Safeguarding Policies and Procedures

The proposal, based on guidance issued by the federal bank regulators, would require securities firms to develop, implement and maintain a comprehensive "information security program" appropriate to the institution's size and complexity, the nature and scope of its activities, and the sensitivity of any personal information. ABASA generally supports the incorporation into Regulation S-P of such an information security program. However, we have significant concerns about the specific requirements specified below.

a. Proposed Definition of "Substantial Harm or Inconvenience to Any Customer"

In accordance with Title V of GLBA, banking organizations and securities firms must have policies and procedures designed to "…protect against unauthorized access to or use of personal information that could result in substantial harm or inconvenience to any customer."[5] The proposal would define the phrase "substantial harm or inconvenience" to include

> [*P]ersonal injury, or more than trivial financial loss*, expenditure of effort or loss of time including theft, fraud, harassment, impersonation, intimidation, damaged reputation, impaired eligibility for credit, or the unauthorized use of the information identified with an individual to obtain a financial product or

[3] 73 *Federal Register* 13692 at 13693. We also note the Commission's concern with "pump and dump" schemes and "phishing" attacks that may lead to account takeovers. While such scams may result in harm to customers, we believe that they are not the result of data breaches at securities firms. Rather, they occur when customers are tricked into revealing their own account access information to the fraudsters. As such, we believe these types of schemes should not be covered by the proposed security breach notice provisions of Regulation S-P.

[4] *Id.* At 13694.

[5] See 17 CFR 248.30, Procedures to safeguard customer records and information.

service, or to access, log into, effect a transaction in, or otherwise use the individual's account." [6]

ABASA strongly urges the Commission to narrow the proposed definition of "substantial harm or inconvenience." The commercial banking industry has long been a target for cyber thieves. We have found, particularly with respect to security breaches in the retail environment, that each breach is different, and that it is difficult to define in a universal fashion when a breach is of a magnitude that it will either cause "substantial harm" or be "trivial" enough not to trigger a breach notification requirement. We do not believe that *every* personal injury rises to the level of substantial harm, as would be dictated by the proposal. Moreover, we believe that the low threshold set by including as "substantial harm" any expenditure of effort or loss of time that is "more than trivial" will lead to subjective, uncertain and inconsistent determinations by securities firms with the potential for criticism by regulators after the fact. Accordingly, ABASA urges the Commission to revise the definition of "substantial harm or inconvenience" to mean a "significant personal injury, financial loss, expenditure of effort or loss of time."

Finally, ABASA agrees that unintentional delivery of an individual's account statement to an incorrect address or changing an individual's account number or password does not constitute "substantial harm."

b. Employee Coordinator Designation

The proposal would also require institutions to designate, in writing, an employee(s) to coordinate the information security program.[7] While ABA agrees that it is important that someone in every institution be held accountable for the information security program, in view of the dynamic nature of the industry, ABASA recommends that securities firms be permitted to make these designations by position or office, rather than designating a specific individual.

c. Proposed Definition of Service Provider

The preamble to the proposal clearly demonstrates the Commission's presumption that the definition of "service provider" would include affiliates of financial institutions thus requiring securities firms to be responsible for (1) ensuring that their affiliates maintain appropriate safeguards through written contracts, and (2) overseeing the affiliate's implementation, maintenance, evaluation, and modifications of appropriate safeguards for the personal information of the securities firms' customers.[8] Bank and financial holding company affiliates are subject to statutory and regulatory provisions, including Sections 23A and 23B of the Federal Reserve Act, that require written contracts between banks and their affiliates. To avoid duplicative effort, we request that amending such contracts to include Regulation S-P requirements be deemed to satisfy the regulation.

ABASA agrees that the use of third-party reviews, including Statements of Auditing Standards No. 70 and a SysTrust report, may be used to evaluate the information safeguards of service providers. However, we urge the Commission to clarify that any *reasonable* method of evaluating service provider safeguards is permissible under the regulation.

---

[6] See proposed paragraph (d)(12) of Section 30.
[7] See proposed paragraph (a)(3)(i) of Section 30.
[8] 73 *Federal Register* 13692 at 13696.

2. Amended Scope of Information/Persons Covered by Safeguarding Requirements

The proposal would expand the scope of persons whose information must be safeguarded to include "any consumer, employee, investor or securityholder who is a natural person." The proposal would further incorporate in information security programs procedures for responding to incidents and unauthorized access to or use of "sensitive personal information" including:

- Notice to affected individuals if misuse of "sensitive *personal* information" has occurred or is reasonably possible; and
- Notice to the Commission when either:
    - A victim of the data breach has suffered substantial harm or inconvenience; *or*
    - An unauthorized person has intentionally obtained access to or used sensitive personal information whether or not any customer has been harmed.

The proposal would also establish a new Form SP-30 to report such notices to the Commission.

ABASA generally supports the adoption of data breach response programs. ABASA believes, however, that the proposal to expand the persons covered by safeguarding requirements exceeds the authority granted to the Commission under Title V of GLBA. In addition, we believe the definition of "sensitive personal information" is so broadly constituted as to be impractical and unworkable.

a. Expanded Scope of Individuals Covered by Safeguarding Requirements

The proposal would expand the scope of the information security program to encompass not only "customers," but also "any consumer, employee, investor or securityholder who is a natural person." However, section 501 of GLBA limits the safeguarding requirement for nonpublic personal information solely to customers.[9] All bank and financial holding companies strive to protect all nonpublic personal information in their possession as a matter of course. And, while it may be laudable to seek to protect through rulemaking the nonpublic personal information of other categories of persons whose information securities firms may possess, it is inappropriate for the Commission to seek to do so through rulemaking in the absence of legislative authority. Accordingly, ABASA strongly opposes this expanded scope.

The Commission seeks comment on further expanding the scope of the safeguarding requirements to non-natural persons, such as corporate clients. Because Title V of GLBA applies only to customers who obtain financial services primarily for "personal, family or household purposes," non-natural persons clearly fall outside the scope of Title V. As above, it is inappropriate for the Commission to expand the scope of the safeguarding provisions through rulemaking.

b. Expanded Definition of "Sensitive Personal Information"

The proposal first would define the term "personal information" to include "any record co*ntaining consumer report information*, or nonpublic personal information." It would then incorporate the term

[9] GLBA and its implementing regulations distinguish between customers and consumers, and it is clear that the Act's safeguarding provisions only cover customers. *See,* 15 U.S.C. § 6801.

"sensitive personal information" into the data breach provisions, as opposed to the term "sensitive *customer* information" which is used in the guidance issued by the FFIEC.[10]

As a practical matter, this broad definition of "personal information" means that virtually all information a securities firm possesses about a given customer becomes "sensitive personal information." Thus, the notice provisions will be triggered when a firm believes misuse of *any* information about a customer is possible, resulting in many more notices to customers. The burden imposed on securities firms by this overbroad definition will be substantial, and the frequency of notices may actually serve to diminish customer response to real threats to their personal information.

In addition, the new term includes as "sensitive personal information" an individual's Social Security number. This is inconsistent with the FFIEC guidance, which only includes a Social Security number as sensitive customer information if compromised *in conjunction* with other information.[11] We have similar concerns about the use of a mother's maiden name unless it is used as an account password or for identification purposes. ABASA believes that a customer's account cannot be accessed merely because someone is aware of a Social Security number or mother's maiden name without any other knowledge to identify the account or its owner. Accordingly, ABASA recommends that the Commission clarify that these two identifiers are sensitive personal information only if compromised with other information that identifies the account or the account owner.

c. Notice to Individuals

In the event that customer sensitive personal information is maintained or otherwise accessible to a service provider and accessed by an unauthorized person, the proposal is not clear as to which party is responsible for providing notice to the affected customers, or whether each party has an independent duty to provide the notice. ABASA recommends that in such circumstances the Commission expressly provide that only one entity need provide notice of the breach.

ABASA believes that the entity on whose behalf the non-public personal information was collected should be deemed the "owner" of such information and should control who has responsibility for providing notice. In addition to being consistent with state breach laws,[12] we believe the owner of the information is in the best position to determine the most efficient and least confusing way to notify individuals. It is not unusual for an institution's use of an external third-party supplier to be transparent to their customers. For example, if a breach occurs at a service provider with which the affected individuals would have had no direct contact – or even be aware of – the securities firm

---

[10] "Sensitive personal information" is defined in the proposal as "any personal information or any combination of components of personal information, that would allow an unauthorized person to use, log into, or access an individual's account, or to establish a new account using the individual's identifying information, including the individual's Social Security number, or any one of the individual's name, telephone number, street address, e-mail address, or online user name, in combination with any one of the individual's account number credit or debit card number, driver's license number, credit card expiration date or security code, mother's maiden name, password, personal identification number, biometric authentication record, or other authenticating information." 73 *Federal Register* 13692 at 13698.

[11] *See,* FFIEC *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice*, March 23, 2005. "Sensitive customer information" is defined as "a customer's name, address, or telephone number, *in conjunction with* the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account."

[12] This approach is consistent with that taken under state breach laws. *See, e.g.,* Section 4-110-105 of the Arkansas Code and California Civil Code Section 1798.82.

may elect to send the notice because of their customers' familiarity with them. Notices sent by an unknown entity would likely confuse customers.[13]

ABASA recommends that the Commission specify that the owner of the information is responsible for either (1) sending the notice, or (2) for establishing the process to determine how such decision will be made in the event of a breach.

Finally, the proposal would require firms to maintain a written record each time personal information may have been accessed or misused. To avoid undue burden, ABASA recommends that firms *not* be required to document instances in which it is determined that personal information has *not* been misused or that misuse is not reasonably possible.

d. Data Security Breach Form SP-30

ABASA believes that the proposed adoption of security incident reporting Form SP-30 is both unworkable from a practical perspective and raises significant important issues concerning the possible release of a securities firm's confidential business information. Importantly, the form requires notice to the Commission as soon as possible with a level of specificity that simply may not be available immediately after a breach is discerned. As a result, the form would have to be updated repeatedly as additional information became available. ABASA believes that the Commission would be better served by adopting the policies and requirements that the federal banking agencies have used with success.

In general, the FFIEC agencies have delegated the process of incident reporting to field offices, with the institution and the field office coming to a mutual determination of how best to report such incidents. The process, as well as the level of reporting, thus varies depending on the institutions' size and location.

ABASA believes it will be easier and more cost effective if the rule permits firms to contact regulators by various means, including by telephone, and generally states the types of information that financial institutions should consider providing rather than specifying a particular form and its contents. Some financial institutions provide tabular data on a periodic basis to their FFIEC agency field offices and have found that to be a useful format. Other institutions, particularly smaller entities, use their own forms.

Because, as noted previously, each security breach is different, ABASA recommends that the Commission give institutions and the Commission's regional offices the opportunity to discuss and agree upon individual reporting formats and not set numerical limits on when incidents are to be reported. In some cases, incidents impacting a small number of customers can be just as important as larger breaches. The flexibility of the FFIEC incident reporting process lends itself to breaches being reported more swiftly, with the information relevant only to that breach, and without regard to a potentially artificial numerical threshold.

In addition to our concerns about the timing required for submitting Form SP-30, ABASA has significant concerns that the information the Commission has specified to be reported on Form SP-30 is confidential business information that should not be made available to the public because it could place the affected firm at a competitive disadvantage. For example, the form requires

[13] If a securities firm delegates sending notices to the service provider, we presume that the firm would be obligated to make sure that the service provider sends such notices in compliance with the rule's requirements.

disclosure of the details concerning the incident, including the personal information compromised and persons involved. We believe that the proposed contents would require disclosure of very sensitive and confidential information, including the covered institution's internal processes and supplier information, which should not be subject to public disclosure.

To the extent a service provider is involved, the form requires details relating to the service provider, including identification of the service provider, services provided and description of involvement in the incident. In some instances this information will likely only be available after detailed analysis and resolution of the incident. In the event the initial filing provided information regarding the involvement of a service provider, subsequent investigation may prove otherwise, creating an unacceptable reputation risk to the named service provider with no significant benefit to be derived from such public exposure.

Moreover, although the proposal indicates that Form SP-30 would be accorded confidential treatment to the extent permitted by law,[14] ABASA remains concerned that the information may become publicly available either through the Commission's website, EDGAR or in response to a Freedom of Information Act request. Indeed, the very fact that a filing was made should be treated to utmost confidentiality by both the Commission and the filing institution.

Because of our concerns about the timing for submission of the form and the confidential nature of the business information proposed to be filed, ABASA opposes the use of a particular form with specified contents for notifying the Commission of data breaches. Rather, we believe that the Commission should adopt the current process used by the federal banking agencies, which has proved beneficial for all parties.

3. Proper Disposal of Personal Information

The proposal would add a new provision to the Commission's current disposal rule to require securities firms to document in writing compliance with the proper disposal of personal information.[15] This could be a significant compliance burden if each and every instance of disposal had to be documented. Rather, ABASA believes that an internal or external audit of the institution's disposal procedures is the only practical means to satisfy this requirement. In addition, ABASA recommends that the Commission clarify in the regulation that individual employees are not liable under Regulation S-P for inadvertent improper disposal of nonpublic personal information of customers. Rather, firms should have the flexibility to determine the ramifications of such lapses for their employees through their policies and procedures.

4. GLBA Exception to Permit Departing Representatives to Take Customer Information

The proposal would provide a new exception that would permit departing registered representatives to take certain customer information with them without their firms providing a notice and opt-out to the affected customers. ABASA members conduct their broker-dealer activities using a variety of business models and recognize that different models may well warrant different practices with respect to the movement of customer information. However, our members are uniformly concerned that the amendment *not* be viewed as having any impact on the authority of a firm to establish, and a registered representative to adhere to, policies concerning the taking of any customer

[14] 73 *Federal Register* 13692 at 13698/

[15] See proposed paragraph (b)(1)(ii) of Section 30.

information, including the limited information provided by the exception. Stated affirmatively, firms must be able, through their policies, employment contracts or other mechanisms, to prohibit or to permit the movement of customer information as they see fit, and this fact must clearly and unequivocally be expressed in conjunction with any opt-out provision. Thus, firms that prohibit the movement of customer information could continue to do so, while firms that choose to permit the movement of customer information would be unaffected except that they would not have to provide the notice and opt-out to affected customers.

Although the proposal states that providing such information under this circumstance would unlikely put an investor at serious risk of identity theft, ABASA believes that customer expectations about sharing their financial information with a third party also merit due consideration. This is particularly the case when bank customers comprise all or a significant portion of the affiliated broker-dealer's clients and their primary relationship is with the bank rather than the registered representative. Additionally, securities firms that operate a number of brokerage branch offices may have a policy that accounts are serviced and maintained at the brokerage branch office level, regardless of which registered representative services the accounts. Importantly, in such cases, the customer believes that their accounts belong to, and are serviced by, the particular brokerage branch rather than by any particular registered representative.

ABASA is also concerned that for those firms that prohibit taking customer information, the proposal would make a difficult enforcement process even more challenging. For example, the proposal as written would not limit representatives to taking information about clients with whom they have a current close working relationship, but would allow them to take information about past investors they have served even though a number of years may have elapsed without contact. Thus, it is absolutely critical that any exception clearly set forth the parameters of information that may be passed on as well as stating affirmatively that any exception has no impact on the ability of firms to prohibit sharing of any and all customer information upon departure.

5. Effective Date

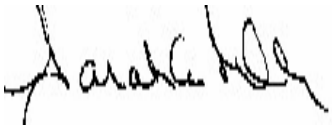
ABASA's members are concerned that the final rule may provide insufficient time to make any necessary systems changes as well as implement the necessary training program. Accordingly, we recommend that the final rule provide for a compliance date at least 18 months after the effective date.

Conclusion

In conclusion, ABASA supports the efforts of the Commission to ensure that customer information is safeguarded and that data breaches are addressed within the limits of its authority under Title V of GLBA. Nonetheless, because integrated bank and financial holding companies have worked diligently to conform their information systems and processes to earlier FFIEC regulations and guidance, we believe that differences between Regulation S-P and FFIEC guidance must be

minimized unless there is compelling evidence that the customer benefits outweigh the costs of retrofitting securities firms" information systems. If you have any questions about the foregoing comments, please contact either the undersigned or Cristeena Naser at 202-663-5332.

Sincerely,



Sarah A. Miller