***Roberta Meyer***
*Vice President & Associate General Counsel*
*(202) 624-2184 t (202) 572-4808 f*
*robbiemeyer@acli.com*

May 12, 2008

Via Electronic Filing

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

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

Ladies and Gentlemen:

The American Council of Life Insurers ("ACLI") is pleased to provide comments to the Securities and Exchange Commission (the "Commission") on its proposed amendments to Regulation S-P, Privacy of Consumer Financial Information and Safeguarding Personal Information.[1] ACLI is the principal trade association of life insurance companies, whose 353 life insurance companies account for 93 percent of the industry's total assets, 93 percent of life insurance premiums and 94 percent of annuity considerations. Many of our member companies manufacture variable annuities and variable life insurance products that are registered under the federal securities laws and distributed through broker-dealers. Over 50% of FINRA's 672,000 registered representatives work for broker-dealers affiliated with life insurance companies. Some life insurance agents also operate as registered investment advisers. Licensed insurance agents that sell variable insurance products are subject to the requirements of both the federal securities laws and state insurance laws. The proposed amendments to Regulation S-P, therefore, will have a significant and distinct impact on life insurers, their distributors, and their agents.

The life insurance industry has long recognized the importance of protecting its customers' nonpublic personal information and strongly supports the confidentiality and safeguarding provisions of the Gramm-Leach-Bliley Act ("GLBA") and implementing state laws and regulations. Our member companies work hard to ensure the confidentiality and security of customer information in accordance with these laws. ACLI appreciates the Commission's efforts to review and revise Regulation S-P standards for safeguarding customer records and responding to data security breaches.

[1] 73 *Fed. Reg.* 13692 (March 13, 2008).

ACLI strongly agrees with the Commission's view that an information security program should be appropriate to the firm's size and complexity, nature and scope of activities and sensitivity of personal information at issue. ACLI believes it is important that a diversified financial organization that includes life insurers be permitted to adopt an information security program that applies to all companies within the organization. This will ensure that the security of the nonpublic personal information of all of the organization's customers is subject to the same level of security protection; and it will appropriately enable the organization to take advantage of economies of scale by adopting information security programs across the entire consolidated organization.

For the reasons just described, ACLI also believes that the proposed requirements for an information security program and response program in the event of security breaches should not conflict with or extend beyond the requirements of Section 501 of the GLBA, the Federal interagency guidance, and applicable state laws and regulations. Accordingly, ACLI urges the Commission to modify the proposed rule as discussed below and as otherwise necessary to achieve this goal. ACLI also requests that the proposed rule be modified to make it clear it is only applicable to information of customers with securities products and does not apply to insurance files maintained separately.

***Proposed GLBA Exception for Disclosures to Departing Brokers, Dealers or Investment Advisers***

The Commission proposes to establish an exception to the GLBA to permit disclosure of certain limited customer information to a broker, dealer or investment adviser, when he or she leaves the company to join another organization, without the need to provide the customer with notice and an opportunity to opt-out from the disclosure. This exception would permit the former representative to solicit customers to whom the representative personally provided a financial product or service on behalf of the company. The information that may be disclosed is limited to the customer's name, contact information (address, telephone number and e-mail address) and a general description of the type of account and products held by the customer. The information may not include the customer's account number, Social Security number or securities positions.

ACLI believes that as written, the exception could be misconstrued to *require* a company to disclose the information specified in the exception to departing representatives. Accordingly, we strongly urge that the rule be clarified to indicate that the exception is not intended to impose *any* requirement that information be disclosed to departing brokers, dealers or investment advisers. In addition, we urge the Commission to underscore that: (i) in any event, the customer information a company's representative may take when departing is governed by the contract between the representative and the company; and (ii) a company's disclosure policies and practices may be subject to other laws or regulations, such as state GLBA privacy laws applicable to insurers, that also govern permitted disclosures by the company. These clarifications are particularly important to our member company life insurers that have registered representatives that are also licensed insurance agents, subject to the requirements of both the federal securities laws and state insurance laws, as well as to obligations and responsibilities under contracts between the parties.



***American Council of Life Insurers***
*101 Constitution Avenue, NW, Washington, DC 20001-2133*
***www.acli.com***

***Proposed Requirements for Information Security Programs***

*Extension of Scope*

ACLI objects to the proposed extension of the requirements with respect to information security programs to employees' information. 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.[2] Section 501(b) authorizes the Commission, certain other Federal agencies, and State insurance authorities to establish appropriate standards for financial institutions to insure the security of *customer* information. State laws and regulations that provide guidance for insurers' implementation of the security requirements of GLBA § 501 are based on the Standards for Safeguarding Customer Information Model Regulation, adopted by the National Association of Insurance Commissioners ("NAIC"). Neither the NAIC Model Regulation nor the state laws that track the NAIC Model Regulation apply to employee information. Similarly, there is nothing in § 501 of the GLBA that applies to employee information. Moreover, the guidance of the Federal banking agencies and the Federal Trade Commission does not extend to employee information.[3]

In view of the express language of GLBA § 501, and in order to be consistent with the requirements of the other Federal agencies and the state insurance authorities, ACLI believes the Commission should not extend the scope of the proposed rule to employee information. Accordingly, the ACLI requests the Commission to adjust the proposed amendment to the definition of "personally identifiable financial information" in § 248.3(u)(1)(iv) and the proposed language of § 248.30(a)(2)(iii), relating to the objectives of an information security program, and to make any other necessary corresponding adjustments to the proposed rule to eliminate any extension of the rule to employee information.

*Definition of Sensitive Information*

The proposed definition of "sensitive personal information" is overly broad and is inconsistent with the definition adopted by the Federal banking agencies. In the proposed rule "sensitive personal information" is defined to mean "personal information." "Personal information" is defined as "any record containing consumer report information, or "nonpublic personal information" as defined in § 248.3(t). As a result, virtually all information a company maintains will be "sensitive personal information." Since the triggers for notice to consumers and regulators are tied to breaches in the security of sensitive personal information, companies will be required to notify customers when misuse of essentially *any* information is reasonably possible and to notify examining authorities when there is a significant risk of substantial harm or inconvenience or an authorized person has intentionally obtained access to or use of essentially *any* information. This is a significant departure from the standards for notice under state security breach laws and used by the other Federal banking agencies, which define "sensitive personal information" in a manner that is far more meaningful to customers.

In addition, ACLI is concerned that the Commission's proposed definition of "sensitive personal information" also includes a person's Social Security Number ("SSN") and the maiden name of the person's mother. The Federal banking agencies regard an SSN as sensitive customer information

[2] 15 U.S.C. § 6801(a).
[3] 70 *Fed. Reg.* 15736 (March 29, 2005).



***American Council of Life Insurers***
*101 Constitution Avenue, NW, Washington, DC 20001-2133*
***www.acli.com***

only if it is used in combination with the individual's name, address or telephone number. ACLI believes that a SSN should be regarded as "sensitive personal information" only if 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 view of the above, ACLI requests the Commission to modify the definition of sensitive personal information in the proposed rule to reflect the definition adopted by the Federal banking agencies.[4]

Further, because the risk of misuse of information that is encrypted or otherwise rendered unreadable through other methods is nonexistent, ACLI believes that information that is rendered unusable through encryption, redaction, or other methods should not be regarded as sensitive personal information unless the confidentiality of the encryption key or other technology has been compromised. Accordingly, ACLI requests that the definition of sensitive personal information also be modified to make it consistent with numerous state security breach laws, that do not treat information as sensitive personal information if the information is encrypted or rendered unusable through redaction or other methods and neither the encryption key nor other technology has been compromised.[5]

*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. The proposed rule states that the term "substantial harm or inconvenience" is defined as "personal injury, or more than trivial financial loss, expenditure of effort or loss of time." ACLI believes that the proposed definition of the term "substantial harm or inconvenience" is appropriate. ACLI agrees with the statement in the proposal that a firm's decision to change to an account number or password is not "substantial harm." ACLI also supports the Commission's statement that unintentional delivery of an account statement to an incorrect address is not substantial harm if the information was unlikely to be misused. ACLI agrees 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. ACLI recommends that these examples be modified so that they also apply to employees of affiliates and service providers.

*Designation of Responsible Employee*

The proposal requests comment on whether companies should be required to designate an employee or employees by name to coordinate the information security program or whether companies should be required to designate a coordinator by position or office. ACLI believes that companies should have the flexibility to decide which option to choose and should be able to have consolidated information security programs. Accordingly, ACLI requests that the Commission permit companies to determine the procedure for designating the appropriate person, position, or area within or across the organization that will have responsibility for coordinating the company's information security program.

---

[4] 70 *Fed. Reg.* at 15752.

[5] *E.g.*, *see* ORS §646A.602(11)(a) (Oregon).



***American Council of Life Insurers***
*101 Constitution Avenue, NW, Washington, DC 20001-2133*
***www.acli.com***

*Service Providers*

Proposed Regulation S-P provides that a company's information security program must require service providers by contract to implement and maintain appropriate safeguards. The definition of service provider includes any entity that is permitted access to personal information through its provision of services to the firm. As a result, the proposed rule appears to require firms that have services provided by affiliates to enter into contracts with their affiliates to implement and maintain safeguards.

ACLI believes that the Commission should not require formal contracts between companies and affiliates that are providing services to them. Requiring formal contractual agreements between affiliates ignores the reality that affiliates generally are subject to company-wide policies and standards relating to safeguarding personal information. Moreover, affiliates typically provide services on an informal basis without a formal contract. In view of the nature of these arrangements, contracts requiring affiliates to implement and maintain appropriate safeguards would appear unlikely to provide additional security protection and unnecessarily burdensome. According, ACLI recommends that the Commission clarify the proposed rule so that contracts are not required under these circumstances.

ACLI agrees that firms should be permitted to 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. ACLI suggests that the Commission also indicate that: (i) other methods for evaluating service provider information safeguards are acceptable as long as they are reasonable, and (ii) formal audits of service providers are not necessary.

***Procedures for Responding to Unauthorized Access or Use - Notice and Form SP-30***

The proposed rule requires companies 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: (i) there is a significant risk of substantial harm or inconvenience to the individual, or (ii) an unauthorized person has intentionally obtained access to or used sensitive personal information.

ACLI believes that notice to the designated examining authority should be required *only* if there is a significant risk that the individual will experience substantial harm or inconvenience; and recommends that the proposed rule be modified accordingly. If an unauthorized person has obtained access to or used sensitive personal information, but there is no significant risk of substantial harm or inconvenience to the individual, no enhanced consumer protection will result from requiring the provision of notice to examining authorities and undue burden will be unnecessarily imposed on companies. Alternatively, the Commission should clarify that "intentionally obtained access to or used sensitive personal information" means to have obtained access to or used the information with intent to commit identity theft or for other unlawful purpose.



***American Council of Life Insurers***
*101 Constitution Avenue, NW, Washington, DC 20001-2133*
***www.acli.com***

ACLI also believes that the proposed Form SP-30 is excessively complex and that its use should not be required The proposed rule requires companies to submit Form SP-30 as soon as possible after becoming aware of an incident of unauthorized access to or use of personal information. Because the form is required to be submitted shortly after the incident has occurred, it is unlikely a company will have all of the information requested in the form.

At a minimum, ACLI urges the Commission to adjust the proposed rule to reflect the approach taken by the Federal banking agencies – which do not require financial institutions to use a specific form and do not specify the details of the filing. ACLI believes that the only information companies should be required to submit to examining authorities is: the name of the company, the date of the incident, a brief description of the incident, the number of persons affected and whom to contact for more information.

ACLI requests that the Commission clarify that: (i) the owner of the information subject to a breach of security is responsible for providing the requisite notices; (ii) only one entity is required to provide the notices; and (iii) a service provider shall provide notice of a breach to the owner of the data. Clarification to this effect is important because in an insurance company offering variable products, there may be one or more investment companies, one or more broker dealers, a transfer agent, and possibly other regulated entities. There is concern that the proposed rule could be construed to require *all* these entities to provide notice.

ACLI also recommends that the proposed rule be modified to require examining authorities to keep confidential and to protect from public disclosure any information they receive in connection with notice of a security breach. ACLI believes that companies should not be required to request confidential treatment with each notice, and that the proposed rule should adjusted to indicate that information provided in filings made with an examining authority, including the Commission, in accordance with Regulation S-P, shall be accorded confidential treatment under relevant laws and rules regarding public availability of information.

***Disposal of Personal Information***

The proposed rule expands the scope and substance of the current provision in Regulation S-P regarding disposal of personal information. ACLI is concerned by the proposed expansion of the Commission's disposal rule well beyond the scope of the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act") and the rules of the other Federal financial institution regulatory agencies. Section 216 of the FACT Act amended the Fair Credit Reporting Act ("FCRA") to require the Federal financial institution agencies to adopt regulations requiring any person that possesses consumer information derived from consumer reports to properly dispose of such information.[6] A consumer report, of course, is a defined term under the FCRA.[7]

When the Commission adopted its disposal rule implementing § 216 of the FACT Act, it applied the rule only to "consumer report information," which is defined as any record about an individual that is or is derived from a consumer report.[8] The same approach was taken by the other Federal

[6] 15 U.S.C. § 1681w.
[7] 15 U.S.C. § 1681a(d).
[8] 17 C.F.R. § 248.30(b)(1)(ii).



*American Council of Life Insurers*
*101 Constitution Avenue, NW, Washington, DC 20001-2133*
*www.acli.com*

agencies when they adopted rules implementing FACT Act § 216.[9] However, the Commission's proposed rule would extend coverage of its current disposal rule to personal information, which, under the proposed rule, includes not only consumer report information, but also any nonpublic personal information about a consumer.[10] Extension of the coverage of the Commission's disposal provisions beyond the scope of the FCRA and the other agencies' requirements will cause the Commission's requirements to be inconsistent with those of the other agencies and will likely impose significant additional burdens on financial institutions without commensurate enhanced consumer protection.

The proposed rule also requires companies to document in writing the proper disposal of personal information. ACLI is concerned that the current language of the proposed rule may be construed to require written documentation of every disposal of documents containing personal information. Again, such a requirement would impose a significant burden and provide questionable additional consumer protection.

In view of the above, ACLI requests that the proposed rule's disposal requirements be modified to be consistent with the Federal banking regulators' rules that extend only to "consumer report information." ACLI also requests that the proposed rule be adjusted to reflect a more reasonable approach that would: (i) require companies to: (a) have appropriate disposal policies and procedures, and (b) periodically review their disposal practices to ascertain whether there is compliance with their policies and required procedures; and (ii) permit companies to rely on certification from their agents or other third parties to the effect that the company is in compliance with its disposal policies and procedures.

***Use of Examples***

ACLI believes that the examples of acceptable practices contained in the *Federal Register* preamble to the proposed rule can be of considerable value to companies because they present real practical situations that firms may encounter. Accordingly, rather than leaving them in a *Federal Register* preamble, ACLI requests that the examples of acceptable practices be incorporated into the final rule as nonexclusive, illustrative examples, that are not prescriptive.

***Internet Authentication and Red Flag Requirements***

The Commission also asks whether the rule's requirements should specify factors such as those identified in the Federal banking agencies' guidance regarding authentication in an Internet environment, or include policies and procedures such as those in the banking agencies' final "red flags" requirements. ACLI does not believe it is necessary for the Commission to adopt these additional requirements and requests that the Commission take no action in this area.

[9] 69 *Fed. Reg.* 77610, 77612 (December 28, 2004).
[10] Proposed Rule § 248.30(d)(8).



*American Council of Life Insurers*
*101 Constitution Avenue, NW, Washington, DC 20001-2133*
*www.acli.com*

***Effective Date***

ACLI believes that member companies may not have sufficient time to implement the rule in an orderly fashion within 60 days after it is adopted. Member companies are likely to need at least eighteen months after the rule is adopted to implement all of the necessary systems changes. Accordingly, we request that the final rule provide that companies will have at least eighteen months after the effective date to implement and comply with the requirements of the rule.

* * *

ACLI appreciates the opportunity to provide its comments on the Commission's proposed amendments to Regulation S-P and appreciates your consideration of its views. If you have any questions, please do not hesitate to contact me

Sincerely,

Roberta Meyer



***American Council of Life Insurers***
*101 Constitution Avenue, NW, Washington, DC 20001-2133*
***www.acli.com***