ROBERTA MEYER
SENIOR COUNSEL, RISK CLASSIFICATION
robbiemeyer@acli.com

A·C·L·I AMERICAN COUNCIL OF LIFE INSURERS
FINANCIAL SECURITY FOR LIFE

31

May 1, 2002

Regulations and Legislation Division
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, N.W.
Washington, DC 20552
Attn: Study on GLBA Information Sharing

Re: Comments on the GLBA Information Sharing Study

Ladies and Gentlemen:

This letter is submitted on behalf of the American Council of Life Insurers (ACLI) in response to the request of the Department of the Treasury (the Department) for public comment on a number of issues to assist the Department in its conduct of the above-referenced study (67 Fed. Reg. 7213 (February 15, 2002)). The ACLI is a national trade association with 399 member life insurance companies representing approximately 76 percent of the life insurance premiums, 75 percent of the annuity considerations, 46 percent of the disability income insurance premiums, and 65 percent of the long term care insurance premiums in the United States among legal reserve life insurance companies. ACLI member company assets account for 75 percent of legal reserve life insurance company assets. The ACLI appreciates being given the opportunity to share its views on the sharing of consumers' personal information. The issues to be addressed in the study are critically important to ACLI member companies as well as their customers.

The businesses of life insurance, annuities, disability income and long term care insurance involve, by their very nature, personal and confidential relationships. At the same time, insurers must be able to obtain, use, and share their customers' personal health and financial information to perform legitimate insurance business functions. These functions are essential to insurers' ability to serve and meet their contractual obligations to their existing and prospective customers. ACLI member companies believe that the sharing of information with affiliates and nonaffiliated third parties generally increases efficiency, reduces costs, and makes it possible to offer innovative products and services to consumers that otherwise would not be available.

Companies which sell life insurance, annuities, disability income and long term care insurance are well aware of the unique position of responsibility they have regarding individuals' personal medical and financial information. ACLI member companies are strongly committed to the principle that individuals have a legitimate interest in the proper collection and handling of their personal information and that insurers have an obligation to assure individuals of the confidentiality of that information. In the last few years, this long held view has been formally reaffirmed by the ACLI Board of Directors through its adoption of "Principles of Support," which relate to the confidentiality of individuals' medical information and the confidentiality of individuals' financial information.

101 CONSTITUTION AVENUE, NW, Suite 700, WASHINGTON, DC 20001-2133
Telephone: (202) 624-2184 Facsimile: (202) 572-4808

The ACLI's Principles of Support in relation to the confidentiality of medical information include, among other things, support for clear prohibitions on insurers' sharing of medical information for marketing purposes or for determination of eligibility for a loan or other credit, even if the insurer and the lender are affiliates. The ACLI's Principles of Support in relation to the confidentiality of financial information reflect the ACLI's strong support for the extensive confidentiality and security protections provided by Title V of the Gramm-Leach-Bliley Act (GLBA). (Copies of the ACLI's Principles of Support are attached to this letter.)

As an industry, life, disability income, and long term care insurers have a long history of maintaining the confidentiality and security of highly sensitive personal information, both medical and financial, in a professionally appropriate manner. We are proud of our record as custodians of this information.

Below are the ACLI's responses to the Department's specific questions:

1. **Purposes for the sharing of confidential customer information with affiliates or with nonaffiliated third parties:**

    a. **What types of information do financial institutions share with affiliates?**

    b. **What types of information do financial institutions share with nonaffiliated third parties?**

    Different types of information are shared by insurers for different purposes. The same types of information are generally shared with affiliates and nonaffiliates, depending on the organizational structure and business plan of the insurer and the function(s) which the affiliate or nonaffiliated third party fulfills for the insurer. Confidential customer information is shared by insurers to enable their performance of essential, legitimate insurance business functions. Insurers' continued ability to share information with both affiliates and nonaffiliates for these purposes is essential to their continued ability to serve and meet their contractual and other obligations to their existing and prospective customers.

    Applications for life, disability income, and long term care insurance seek nonmedical information, such as age, occupation, income, net worth, social security number, and other insurance and beneficiary designations. Applications for these products also include other questions which focus on the proposed insured's health, including current medical conditions, past illnesses, injuries and medical treatments. Often the applicant will be asked to provide the name of each physician or practitioner consulted in connection with any ailment within a specific period or time (typically five years). Depending on the age and medical history of the proposed insured and the amount of coverage applied for, medical record information or additional financial information may be required.

    The medical information that insurance companies typically request of applicants includes routine measurements, such as height and weight, blood pressure, and cholesterol level. The insurer may also seek an evaluation of blood, urine or oral fluid specimens, including tests for tobacco or drug use or HIV infection. Since life, disability income, and long term

care insurance policies are long range financial products purchased to provide financial security, it is often necessary for the insurer to also assess and use personal financial information, such as occupation, income, net worth, assets, and estate planning goals.

The nature and amount of information obtained by insurers at the inception of annuity contracts varies based on whether the product sought is a fixed, variable, single, or multiple premium annuity. An insurer may seek the annuitant's name, address, social security number, and, depending on the type of annuity being applied for, various information relating to his or her income, assets, financial needs, or estate planning goals.

During the lifetime of a life insurance policy, an annuity, and a disability income or long term care insurance policy, the insurer also develops additional customer information which relates to particular insurance contracts and which emanates from the insurance relationships themselves. Information of this nature includes, for example, the value of a variable death benefit, the value of various policy accounts, such as separate or variable accounts, cash surrender values, loan values, and the name of new beneficiaries.

An insurer will limit access to an individual's personal health or financial information which is in its possession.. However, the insurer must use and share that information with affiliates and nonaffiliated third parties in order to perform legitimate, essential insurance business functions, such as those described in Section 502(e) of GLBA – to underwrite the applications of prospective customers, to pay claims, to administer and service existing contracts with existing customers, and to perform related product or service functions.

Insurers that provide life insurance, annuities, and disability income and long term care insurance must share personal customer information in order to comply with various regulatory/legal mandates and in furtherance of certain public policy goals (such as the detection and deterrence of fraud). Activities in connection with ordinary proposed and consummated business transactions, such as reinsurance treaties and mergers and acquisitions, also necessitate insurers' sharing of customer information.

Insurers also share limited customer information with affiliates and nonaffiliates for marketing purposes. This enables them to inform consumers of `new products and services that may be of particular interest to them. It makes it possible for insurers to tailor products and services that recognize and respond to individuals' particular needs and to avoid inundating consumers with information about products and services that will not benefit nor interest them.

c. Do financial institutions share different types of information with affiliates than with nonaffiliated third parties? If so, please explain the differences in the types of information shared with affiliates and with nonaffilated third parties.

Insurers generally share the same types of information with both affiliates and nonaffiliates.

d. For what purposes do financial institutions share information with affiliates?

e. For what purpose do financial institutions share information with nonaffiliated third parties?

Insurers use affiliates and nonaffiliated third parties in connection with the performance of essential, core functions associated with an insurance contract. Insurers share personal customer information with affiliates and nonaffiliates so that they may fulfill these functions.

It is quite common for insurers to use affiliates or nonaffiliated third parties to perform basic insurance business functions such as underwriting, claims evaluation, and policy administration. Insurers also use affiliates and nonaffiliated third parties to perform important functions, not necessarily directly related to a particular insurance contract, but essential to the administration or servicing of insurance policies generally, such as, for example, for development and maintenance of computer systems.

Third parties, such as actuaries, physicians, attorneys, auditors, investigators, translators, records administrators, third party administrators, employee benefits or other consultants, and others are often used to perform business functions necessary to effect, administer, or enforce insurance policies or the related product or service business of which these polices are a part. Often these arrangements with affiliates or nonaffiliated third parties provide the most efficient and economical way for an insurer to serve prospective and existing customers. The economies and efficiencies devolving from these relationships inure to the benefit of the insurer's customers.

Insurers which sell life insurance, annuities, and disability income and long term care insurance also must regularly disclose personal information to: (1) state insurance departments as a result of their general regulatory oversight of insurers, which includes regular market conduct and financial examinations of insurers; (2) self-regulatory organizations, such as the Insurance Marketplace Standards Association (IMSA), which imposes and monitors adherence to requirements with respect to member insurers' conduct in the marketplace; and (3) state insurance guaranty funds, which seek to satisfy policyholder claims in the event of impairment or insolvency of an insurer or to facilitate rehabilitations or liquidations which typically require broad access to policyholder information.

Furthermore, insurers need to (and, in fact, in some states are required to) disclose personal information in order to protect against or to prevent actual or potential fraud. Such disclosures are made to law enforcement agencies, state insurance departments, the Medical Information Bureau (MIB), or outside attorneys or investigators, which work for the insurers. Additionally, they must also be able to meet requirements established under the USA Patriot Act, Pub. Law 107-56 (USA Patriot Act).

In the event of a proposed or consummated sale, merger, transfer, or exchange of all or a portion of an insurance company, it is often essential that the insurer disclose company files. Naturally, these files contain personal information. Such disclosures are often necessary to the due diligence process which takes place prior to consummation of the transaction and are clearly necessary once the transaction is completed when the resulting entity often must use policyholder files in order to conduct business.

Insurers also frequently enter into reinsurance contracts in order to, among other things, increase the nature and amount of coverage they can make available to consumers. These arrangements often necessitate the disclosure of personal customer information by the primary insurer to the reinsurer. Depending on the particular reinsurance treaty, this might happen because the reinsurer: (1) wishes to examine the ceding insurer's underwriting practices; (2) actually assumes responsibility for underwriting all or part of the risk; or (3) administers claims for an insurer.

As noted above in response to questions #1.a. and #1.b., insurers also use and share limited customer information with affiliates and nonaffiliates for marketing purposes in order to tailor their marketing communications to consumers most likely to be interested in and to benefit from particular new products or services.

f. What, if any, limits do financial institutions voluntarily place on the sharing of information with their affiliates and nonaffiliated third parties? Please explain.

The sharing of nonpublic personal information by insurers is subject to the limitations on reuse of the information imposed under GLBA and related federal and state laws and regulations. In addition, once insurers obtain personal customer information, it is used internally and shared with affiliates and nonaffiliates on a "need to know" basis. In other words, a business purpose is generally required for the sharing of information. For example, one ACLI member company advises that its agents do not have access to its underwriters' files and vice versa, unless one or the other establishes a business need to access the other's file.

Some ACLI member companies have erected firewalls between different divisions of single companies and between affiliates to prevent unnecessary sharing of information. Other member companies use encryption or require use of passwords for the sharing of information between affiliates for the same reason.

Also, some ACLI member companies put "flags" on the files of certain individuals to prevent the sharing of personal information where the individuals have opted-out of the sharing of their information with either affiliates or nonaffiliates, have requested that their personal information not be used for certain purposes or have indicated that they do not wish to receive certain marketing information.

g. What, if any, operational limitations prevent or inhibit financial institutions from sharing information with affiliates and nonaffiliated third parties? Please explain.

h. For what other purposes would financial institutions like to share information but currently do not?

The major obstacle to insurers sharing information with nonaffiliated third parties arises from individual states' enactment or promulgation of legislation or regulations that depart materially from the GLBA Title V standards. Insurers are concerned that states such as New Mexico and Vermont have imposed burdens on insurers that inhibit their ability to serve and provide innovative products and services to consumers without increasing privacy protection. If this trend continues, we believe that the balkanization of privacy laws by individual states will present considerable obstacles for insurers and their ability to serve consumers. The ACLI has long maintained and continues to believe that a single, preemptive national privacy standard would provide clarity and economies to both consumers and insurers.

In addition, ACLI member companies are very concerned that the rule recently proposed by the Treasury Department to implement § 314(b) of the USA Patriot Act will have the effect of deterring insurers from sharing information about suspected terrorists and money launderers with other financial institutions. This concern arises because insurers are not defined as financial institutions under the proposed rule. We urge the Treasury to include insurers within the scope of the final rule which implements § 314(b).

2. The extent and adequacy of security protections for such information:

a. Describe the kinds of safeguards that financial institutions have in place to protect the security of information. Please consider administrative, technical, and physical protections, as well as the protections that financial institutions impose on their third-party service providers.

ACLI member companies comply with the security requirements of Section 501 of GLBA and the implementing security regulations of the federal banking regulators, where applicable. Those member companies licensed in New York comply with New York Regulation No.173. Also, the National Association of Insurance Commissioners (NAIC) has recently adopted a model state regulation providing guidance for insurers' implementation of the security requirements of GLBA Section 501. ACLI member companies will be subject to this model once it is adopted in the various states.

It is noteworthy that insurers successfully protected the security of their customers' personal information long before they were required to do so by GLBA or its implementing regulations. Over the years, insurers have developed many different ways of ensuring the security of personal customer information. Some of the practices currently used by ACLI member companies include the following:

Company employees with access to confidential customer information are often required to undergo special training and to adhere to privacy principles and rules of conduct. They are required to adhere to many different types of requirements designed to protect the physical security of customers' information. For example, employees generally may only disclose customer information to others on a "need to know" basis. They are required to lock confidential files, to clear off their desks before going home, and to use special passwords to access customer information. Similar confidentiality and security principles are applied to member company agents and brokers who are also given instruction.

Generally, ACLI member companies subscribe to a philosophy wherein access to information is denied unless otherwise required by defined business needs. Often full-time staffs of security professionals design, implement and maintain multi-layered security systems that are designed to protect the integrity and confidentiality of customer records and information.

Some member companies limit access to their buildings by requiring use of key cards and badges to enter. Many have erected various forms of firewalls between different divisions of a single company. Some use various forms of encryption. Some have imposed limits on the use of e-mails for certain purposes. Others have developed special intranets for internal communications in order to protect against hackers. Some member companies have virtual service centers requiring the use of various different passwords to access the system. Others employ a PIN process in connection with the provision of customer service.

Some member companies control access to information through use of security systems on computing platforms. Users are variously authenticated by means of logon ids and/or secret passwords. In some cases, digital certificates are also used for purposes of authentication and non-repudiation, access control lists limit levels of access based on customer profiles or employee job functions, and formal data classification schemes facilitate the application of security provisions commensurate with the level of sensitivity of any given body of data so that sensitive date is stored only on secure platforms.

Some companies also use intrusion detection systems to monitor network traffic for indications of attempted break-ins. When pre-established thresholds are exceeded, automated systems send messages via e-mail and/or pagers to security professionals for immediate follow-up. Event logs, violation reports and other types of electronic "footprints" are reviewed on a periodic basis for indications of potential wrongdoing.

Because information technology continues to evolve, ACLI member companies monitor all significant alert services for new vulnerabilities and hazards. Ties to law enforcement and

industry experts are maintained as further assurance that emerging threats will be recognized and that counter measures will be deployed in a timely manner.

b. To what extent are the safeguards described above required under existing law, such as the GLBA (*see, e.g.*12 CFG 30, Appendix B)?

Most of the safeguards described above have been voluntarily implemented by insurers to protect the security of their customers' information. Many, if not most, of these safeguards were put into place before and without regard to whether there was any legal requirement to do so under the GLBA or any other law. As a result, the imposition of the requirements of GLBA Section 501 and its implementing regulations was consistent with ACLI member companies' historic and ongoing efforts to protect the security of their customers' personal information.

c. Do existing statutory and regulatory requirements protect information adequately: Please explain why or why not.

d. What, if any, new or revised statutory or regulatory protections would be useful? Please explain.

Given the breadth of the safeguards described above and the security requirements imposed under GLBA and its implementing rules and regulations, there can be no doubt that insurers' personal customer information is adequately protected. No new or revised statutory or regulatory protections are needed to ensure the security of personal customer information, except as may be necessary to fulfill the requirements of the USA Patriot Act. Though insurers may require additional statutory or regulatory protections due to the requirements of the USA Patriot Act, specific suggestions currently cannot be made because the insurance regulations under the USA Patriot Act have not as yet been issued by the Treasury Department. After those regulations are issued, the ACLI may have additional suggestions, and respectfully reserves the right to make such additional suggestions at that point in time.

3. The potential risks for customer privacy of such sharing of information:

a. What, if any, potential privacy risks does a customer face when a financial institution shares the customer's information with an affiliate?

The ACLI does not believe that there are privacy risks posed by an insurer's sharing of a customer's information with an affiliate. The federal Fair Credit Reporting Act (FCRA) governs and imposes requirements in relation to the sharing of customers' information among affiliates. Moreover, customer information shared by insurer financial institutions with their affiliates is provided in connection with the performance of ordinary business activities. Such sharing enables the performance of these functions in the most efficient and economic way possible and permits beneficial tailoring of marketing communications to consumers.

b. What, if any, potential privacy risks does a customer face when a financial institution shares the customer's information with a nonaffiliated third party?

c. What, if any, potential risk to privacy does a customer face when an affiliate shares information obtained from another affiliate with a nonaffiliated third party?

The ACLI does not believe that privacy risks are posed by the sharing of customers' personal information with nonaffiliates under either of the scenarios described above. GLBA Section 502(c) limits the reuse of information received by a nonaffiliated third party from a financial institution and prohibits further disclosure of such information to "... any other person that is a nonaffiliated third party of both the financial institution and such receiving third party, unless such disclosure would be lawful if made directly to such other person by the financial institution." Accordingly, nonaffiliated third party recipients of nonpublic personal information from an insurer or an affiliate of an insurer are, in effect, subject to the breadth of the broad privacy requirements provided under the GLBA.

Most information shared by financial institution insurers with nonaffiliates is shared to facilitate the performance of core insurance business functions. Moreover, under GLBA Section 502(b)(2), if there is disclosure of confidential customer information to a nonaffiliated third party service provider or pursuant to a joint marketing agreement, the insurer must not only fully disclose to the customer the sharing of such information, but also must enter "into a contractual agreement with the third party that requires the third party to maintain the confidentiality of such information."

4. The potential benefits for financial institutions and affiliates of such sharing of information (specific examples, means of assessment, or evidence of benefits would be useful.)

a. In what ways do financial institutions benefit from sharing information with affiliates?

b. In what ways do financial institutions benefit from sharing information with nonaffiliated third parties?

As noted at the outset of this letter, ACLI member companies believe that sharing of customer information by insurers with affiliates and nonaffiliated third parties is critical to insurers' performance of fundamental insurance business functions. Such sharing, discussed in detail above in response to question #1, generally increases efficiency, reduces costs, and makes it possible for insurers to offer economies and innovative products and services to consumers that otherwise would not be available.

The sharing of customer information by insurers with affiliates makes it possible to, for example, combine data systems and operations and, as a result, to acquire information more cost effectively, to avoid the costs of maintaining redundant systems, and to consequently expend fewer resources. Information sharing with nonaffiliated third parties

allows financial institution insurers to outsource many basic insurance business operations, including underwriting and claims administration, and records management. Integrated data systems and third-party contractors offer enhanced services, customer convenience, and lower costs. These arrangements with affiliates and nonaffiliated third parties often provide the most efficient and economical way for an insurer to serve prospective and existing customers. The economies and efficiencies devolving from these relationships inure to the benefit of the insurer's customers.

The sharing of customer information by financial institutions with affiliates and nonaffiliates for marketing purposes enables financial institutions to tailor products and services that recognize and respond to individuals' particular needs and to inform consumers most likely to be interested in particular new products and services. Such targeted marketing permits insurers to avoid sending information to people about products and services unlikely to be of interest to them.

c. In what ways do affiliates benefit when financial institutions share information with them?

d. In what ways do affiliates benefit from sharing information that they obtain from other affiliates with nonaffiliated third parties?

Under both sets of scenarios described above, it would seem that affiliates of insurers generally would derive the same sorts of economies and efficiencies that insurers derive from the sharing of customer information.

e. What effects would further limitations on such sharing of information have on financial institutions and affiliates?

Further limitations on the sharing of customer information by insurers would jeopardize the performance of fundamental and legitimate insurance business functions described above. They would jeopardize the increased efficiency, the reduced costs, the 24-7 service, and the innovative products and services that sharing now makes possible. The resulting limitations on insurers' marketing practices would inhibit insurers' ability to tailor products and services that recognize and respond to individuals' particular needs and avoid bothering them with information about products and services unlikely to be of interest.

5. The potential benefits for customers of such sharing of information (specific examples, means of assessment, or evidence of benefits would be useful):

a. In what ways does a customer benefit from the sharing of such information by a financial institution with its affiliates?

b. In what ways does a customer benefit from the sharing of such information by a financial institution with nonaffiliated third parties?

c. In what ways does a customer benefit when affiliates share information they obtained from other affiliates with nonaffiliated third parties?

The sharing of personal customer information by insurers with both affiliates and nonaffiliates enables the performance of fundamental and legitimate insurance business functions. It enhances efficiency, reduces costs, makes possible 24-7 customer service, and the marketing of individually tailored, innovative products and services. Insurers' arrangements with affiliates and nonaffilated third parties often provide the most efficient and economical way for an insurer to serve prospective and existing customers. The economies and efficiencies devolving from these relationships inure to the benefit of the insurer's customers.

Insurers' current ability to share customer information with affiliates and nonaffiliated third parties increases the speed with which insurers may issue new insurance policies and service existing policies. The sharing of information across affiliates facilitates consolidated statements and comparison shopping for insurance. Disclosures to state insurance departments, self regulatory organizations, and state guaranty funds enhance consumer protection against insurer insolvencies and the payment of consumer claims in the event of insolvencies. The sharing of information to deter and prevent fraud saves consumers untold costs of fraud.

Information sharing makes possible a vibrant reinsurance market. This permits broader sharing of previously unacceptable risks and enables many Americans who were previously thought uninsurable or who could not previously afford life, disability income, and long term care insurance to obtain coverage.

Responsible information sharing enables insurers to identify and market their products and services to individuals likely to benefit from particular products and services. Similarly, it permits insurers to avoid contacting consumers about products and services unlikely to meet their particular needs.

Perhaps most importantly, the economies, efficiencies, and product and service innovations made possible by information sharing have enhanced the availability of insurance products to middle and lower middle income Americans. In sum, information sharing has significantly improved ACLI member companies' ability to serve and to provide products and services to American consumers most in need.

d. What, if any alternatives are there to achieve the same or similar benefits for customers without such sharing of such information?

The ACLI is unaware of alternatives to information sharing which would achieve the same or similar benefits to consumers described above.

e. What effects, positive or negative, would further limitations on the sharing of such information have on customers?

The negative effects of further limitations on sharing on customers, as well as on insurers, are addressed above in response to question # 4.e.

6. The adequacy of existing laws to protect customer privacy:

a. Do existing privacy laws, such as GLBA privacy regulations and the Fair Credit Reporting Act (FCRA) adequately protect the privacy of a customer's information. Please explain why or why not.

The ACLI strongly believes that the privacy of a customer's information is adequately protected under existing federal and state privacy laws and regulations governing insurers' information practices. The multitude of existing federal and state privacy laws and regulations, including the GLBA, the FCRA, the Health and Human Services (HHS) Standards for the Privacy of Individually Identifiable Health Information, the 16-18 statutes tracking the NAIC Insurance Information and Privacy Protection Model Act and the approximately 40 new statutes and regulations tracking the NAIC Model Privacy of Consumer Financial and Health Information Regulation, adopted to implement the GLBA, provide a broad comprehensive regulatory framework to protect the privacy of customer information.

b. What, if any, new or revised statutory or regulatory protections would be useful to protect customer privacy? Please explain.

Given the fact that the privacy requirements of GLBA have only recently gone into effect and their benefits may not yet be fully assessed, coupled with the multitude of existing privacy laws and regulations, described above, the ACLI does not believe that additional privacy protections are now necessary to protect customers' information. However, it is noteworthy that the ACLI has long maintained and continues to believe that a single, preemptive national privacy standard would provide clarity and economies to both consumers and insurers. Along the same lines, ACLI member companies strongly believe that it is absolutely critical that under the current regulatory system, insurers are subject to privacy laws and regulations which are uniform with the laws and regulations to which other financial institutions are subject and at least operationally uniform from state to state.

7. The adequacy of financial institution privacy policy and privacy rights disclosure under existing law:

a. Have financial institution privacy notices been adequate in light of existing requirements? Please explain why or why not.

b. What, if any new or revised requirements would improve how financial institutions describe their privacy policies and practices and inform

customers about their privacy rights? Please explain how any of these new or revised requirements would improve financial institutions' notices.

Insurers, like other financial institutions, undertook massive compliance efforts to meet the notice requirements of GLBA Title V. They spent billions of dollars and sent out billions of notices by the required July 1, 2001 deadline. It was not an easy process. However, the industry has been generally pleased with the results of these notices. Most have been "clear and conspicuous."

At the same time, the ACLI is aware that some issues have been raised with respect to the complexity of the notices. We note that this was a first time effort both for regulators, in drafting detailed requirements and sample clauses for the notices, and for financial institutions, in crafting and delivering their individualized notices. We understand that the required details of the notices sometimes made them long and that the required "legalese" sometimes made them difficult to understand. In addition, in many instances insurers followed the model language and sample clauses developed by federal and state regulators in order to ensure compliance with the GLBA.

In view of the concerns which have been raised with respect to the notices, the ACLI is participating in a working group of the Financial Services Coordinating Council (FSCC) which is exploring various approaches to simplification of the notices. Recognizing the difficulty of developing a simplified, short, "one size fits all" notice for all financial institutions, efforts are likely to be directed at the possibility of development of suggested simplified common terminology and various simplified clauses or provisions which could be deemed acceptable by federal and state regulators, and viewed as "safe harbor" language.

8. **The feasibility of different approaches, including opt-out and opt-in, to permit customer to direct that such information not be shared with affiliates and nonaffiliated third parties:**

    a. **Is it feasible to require financial institutions to obtain customers' consent (opt-in) before sharing information with affiliates in some or all circumstances? With nonaffiliated third parties? Please explain what effects, both positive and negative, such a requirement would have on customers and on financial institutions.**

The ACLI strongly believes that it would not be feasible to require financial institution insurers to obtain customers' consent (opt-in) before sharing customer financial information with affiliates or nonaffiliated third parties under any circumstances. ACLI member companies strongly believe that it would not be feasible to require insurers to obtain customers' consent (opt-in) before sharing customer medical information in connection with the performance of core insurance business functions and related product or service functions, such as those described in GLBA Section 502(e). However, since ACLI member companies do not share medical information (i.e., information as to an individual's past or present physical or mental condition) for marketing purposes and have

adopted a principle of support in favor of a prohibition on the sharing of such information for marketing purposes, they do believe that it would be feasible to require an opt-in as a prerequisite to the sharing of customer medical information (i.e., information as to an individual's past or present physical or mental condition) for marketing purposes.

It is not true that an opt-in provides consumers greater protection than an opt-out. Both opt-in and opt-out give consumers the same level of control over their information, since it is the consumer alone who makes the final decision about use of his or her information. Opt-in is more expensive and the cost is ultimately borne by consumers. Opt-in will result in less targeted marketing of consumers, resulting in their receipt of more information about products and services less likely to be of interest to them. Opt-in will restrict competition and entry into new markets disadvantaging consumers as well as insurers.

Further discussion of the effect of increased limitations on the sharing of customer information is set forth above in response to question #4.e.

b. Under what circumstances would it be appropriate to permit, but not require, financial institutions to obtain customers' consent (opt-in) before sharing information with affiliates as an alternative to a required opt-out in some or all circumstances? With nonaffiliated third parties? What effects, both positive and negative, would such a voluntary opt in have on customers and financial institutions? (Please describe any experience of this approach that you may have had, including consumer acceptance.)

Under current law financial institution insurers may already obtain customers' consent prior to sharing their personal information with an affiliate or a nonaffiliated third party. The ACLI believes that this permissive approach is appropriate and desirable.

c. Is it feasible to require financial institutions to permit customers to opt out generally of having their information shared with affiliates? Please explain what effects, both positive and negative, such a requirement would have on consumers and on financial institutions.

The ACLI strongly believes that it would not be feasible to permit customers to generally opt out of the sharing of their information with affiliates. First, if an individual were to be permitted to "opt out" of an insurer's right to share his or her personal information with an affiliate which performs a core insurance business function for the insurer, it would be extremely difficult, if not impossible, for the insurer to provide that consumer with the coverage, service, benefits, or economies that otherwise would be available.

For example, it is impractical for an individual seeking life insurance coverage from an insurer which uses an affiliate to perform its underwriting to opt out from information sharing. If the individual opts out of the insurer's ability to disclose personal health information to the affiliate, the insurer will not be able to underwrite the policy because it does not have the internal capacity to do. If a policyholder under an existing life insurance policy opts out of the insurer's ability to use or disclose personal health or financial

information, and the life insurer uses an affiliate to process policy loans or claims, the insurer will either not be able to process a policy loan request or claim submitted by that individual.

Finally, the ACLI strongly believes that limitation of the sharing of customer information among affiliates for marketing purposes beyond the limitations already imposed under the FCRA would inhibit sharing within holding company structures which is anticipated by consumers and which enables marketing to consumers of integrated and appropriately tailored products and services.

d. What, if any, other methods would permit customers to direct that information not be shared with affiliates or nonaffiliated third parties? Please explain their benefits and drawbacks for customers and for financial institutions of each method identified.

The ACLI is not aware of other methods which would permit customers to direct that information not be shared with affiliates or nonaffiliated third parties.

9. **The feasibility of restricting sharing of such information for specific uses or of permitting customers to direct the uses for which such information may be shared:**

   a. **Describe the circumstances under which or the extent to which customers may be able to restrict the sharing of information by financial institutions for specific uses or to direct the uses for which such information may be shared.**

   b. **What effects, both positive and negative, would such a policy have on financial institutions and on consumers?**

   c. **Please describe any experience you may have had of this approach.**

   Given the breadth and importance of information sharing to insurers' ability to serve their customers, described throughout this letter, the ACLI strongly believes that it would not be feasible to permit consumers to restrict sharing of information for specific uses or to direct the uses for which such information may be shared other than in connection with the sharing of medical information for marketing purposes as discussed above in response to question # 8.a.

The ACLI appreciates the opportunity to submit these comments, and would be pleased to answer any questions you may have relating to the above comments.

Sincerely,

Roberta B. Meyer
Senior Counsel

Attachment 1

Confidentiality of Medical Information

Principles of Support

Life, disability income, and long-term care insurers have a long history of dealing with highly sensitive personal information, including medical information, in a professional and appropriate manner. The life insurance industry is proud of its record of protecting the confidentiality of this information. The industry believes that individuals have a legitimate interest in the proper collection and use of individually identifiable medical information about them and that insurers must continue to handle such medical information in a confidential manner. The industry supports the following principles:

1. Medical information to be collected from third parties for underwriting life, disability income and long-term care insurance coverages should be collected only with the authorization of the individual.

2. In general, any redisclosure of medical information to third parties should only be made with the authorization of the individual.

3. Any redisclosure of medical information made without the individual's authorization should only be made in limited circumstances, such as when required by law.

4. Medical information will not be shared for marketing purposes.

5. Under no circumstances will an insurance company share an individual's medical information with a financial company, such as a bank, in determining eligibility for a loan or other credit - even if the insurance company and the financial company are commonly owned.

6. Upon request, individuals should be entitled to learn of any redisclosures of medical information pertaining to them which may have been made to third parties.

7. All permissible redisclosures should contain only such medical information as was authorized by the individual to be disclosed or which was otherwise permitted or required by law to be disclosed. Similarly, the recipient of the medical information should generally be prohibited from making further redisclosures without the authorization of the individual.

8. Upon request, individuals should be entitled to have access and correction rights regarding medical information collected about them from third parties in connection with any application they make for life, disability income or long-term care insurance coverage.

9. Individuals should be entitled to receive, upon request, a notice which describes the insurer's medical information confidentiality practices.

10. Insurance companies providing life, disability income and long-term care coverages should document their medical information confidentiality policies and adopt internal operating procedures to restrict access to medical information to only those who are aware of these internal policies and who have a legitimate business reason to have access to such information.

11. If an insurer improperly discloses medical information about an individual, it could be subject to a civil action for actual damages in a court of law.

12. State legislation seeking to implement these principles should be uniform. Any federal legislation to implement the foregoing principles should preempt all other state requirements.

Attachment 2

Confidentiality of Nonpublic Personal Information
Other Than Medical Information
Principles of Support

Life, disability income, and long term care insurers have a long and established history of handling their customers' nonpublic personal information in a professional and confidential manner. Insurers recognize their affirmative and continuing obligation to respect their customers' privacy and to protect the confidentiality and security of their customers' nonpublic personal information.

Insurers support principles in relation to medical information which are described in a separate document. This document sets forth principles which insurers support in relation to nonpublic personal information other than medical information.

1) Requirements with respect to the confidentiality and security of nonpublic personal information should be addressed separately from those in relation to medical information in order to more fully address the different concerns that arise in connection with each type of information.

2) An insurer shall establish and maintain policies and practices designed to protect the confidentiality of nonpublic personal information and to protect against unauthorized access to or use of such information which could result in substantial harm or inconvenience to any customer.

3) An insurer shall establish and maintain policies and practices designed to protect the security of nonpublic personal information against anticipated threats or hazards or unauthorized access to or use of such information which could result in substantial harm or inconvenience to any customer.

4) An insurer shall provide its customers with a notice of the policies it maintains to protect the confidentiality and security of nonpublic personal information. This notice shall be provided at the time the insurer enters into an insurance contract and at least annually thereafter for as long as the contract is in force.

5) In order to serve its prospective and existing customers, an insurer may share its customers' nonpublic personal information in connection with the origination, administration, or servicing of its products or services or to engage in other non-marketing business operations. For example, an insurer may share nonpublic personal information to provide consolidated statements of an individual's different accounts, to prevent fraud, or to comply with the law or a civil or criminal subpoena or summons.

6) An insurer shall not share a customer's nonpublic personal information within its corporate family for marketing products or services unless the insurer's notice says that this information may be shared within its corporate family for this purpose.

7) An insurer shall not share a customer's nonpublic personal information outside its corporate family for marketing unless: (a) the insurer's notice says that nonpublic personal information may be shared by the insurer outside its corporate family for this purpose; and either (b) the customer is given the opportunity to direct that it not be shared; or (c) the products or services to be marketed are: ((1)) products or services of the insurer; or ((2)) offered by the insurer and another financial institution (or institutions) pursuant to a joint agreement.

8) An insurer shall not share a customer's nonpublic personal information with another person or entity unless such party is subject to the same restrictions on disclosure of nonpublic personal information to which the insurer is subject.

9) Upon request, a customer of an insurer is entitled to have access and correction rights regarding nonpublic personal information about the customer collected from third parties in connection with an application for life, disability income, or long term care insurance.

10) In order to provide insurers' customers protection that is as uniform as possible, any legislation or regulation seeking to impose requirements with respect to the confidentiality and security of nonpublic personal information shall be applicable in the same manner to all entities which collect and maintain such information.

11) State legislation seeking to implement these principles should be uniform. Any federal legislation implementing these principles should preempt any state law imposing requirements with respect to the confidentiality and security of nonpublic personal information.