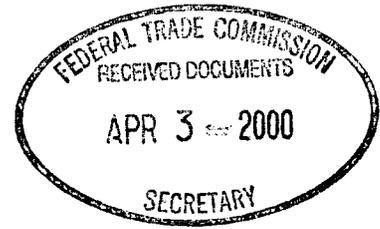


ROBERTA B. MEYER  
SENIOR COUNSEL  
robbiemeyer@acli.com



March 31, 2000

Secretary  
Federal Trade Commission  
Room H-159  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

Re: Proposed Privacy Regulations Under Title V of the Gramm-Leach-Bliley Act

Ladies and Gentlemen:

These comments are submitted on behalf of the American Council of Life Insurers ("ACLI") in response to your request for public comment on your proposed rule implementing the privacy provisions of Title V of the Gramm-Leach-Bliley Act (the "GLB Act"). The ACLI is a national trade association whose 435 member companies represent approximately 73 percent of the life insurance and 87 percent of the long term care insurance in force in the United States. They also represent over 80 percent of the domestic pension business funded through life insurance companies and 71 percent of the companies that provide disability income insurance. The ACLI commends you for your effort in crafting this important rule and appreciates the opportunity to submit these comments.

As insurers, ACLI member companies are not directly subject to the proposed rule. However, we believe that it is important for us to comment on it for several reasons. First, to the extent that member companies affiliate or otherwise enter into business relationships with financial institutions which are subject to your agency's jurisdiction, they will be significantly affected by your rule. In addition, the GLB Act requires the federal agencies to adopt rules that are consistent and comparable. The ACLI has urged the National Association of Insurance Commissioners ("NAIC") to adopt a similar approach with regard to any model rule it may be considering for use at the state level.

We believe it is critically important that any rules adopted by the states be uniform from state to state and that they be consistent with, if not identical to, the rules adopted at the federal level. This is necessary in order to facilitate a smooth implementation of the privacy provisions of the GLB Act, and to avoid undermining the reasons for which it was enacted. It is our hope that the states will use the proposed federal rule as a template in developing state rules. In order to achieve this goal, we are submitting comments which take into account the distinctive business practices and concerns of insurers.

By its very nature, the business of life, disability income and long term care insurance and pensions involves personal and confidential relationships. However, insurers selling these products must be able to obtain, use, and share their customers' personal information, including their nonpublic personal information, in order 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 also believe that the sharing of information with affiliates and nonaffiliated third parties generally increases efficiency, reduces costs, and makes it possible to offer consumers economies and innovative products and services that otherwise would not be available.

ACLI member companies are well aware of their unique position of responsibility in relation to the personal information of their existing and prospective customers. They 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. Toward this end, the ACLI Board of Directors has adopted policy in relation to the confidentiality of medical and nonpublic personal information. This policy is set forth in two sets of "Principles of Support" – one in relation to medical information; the other in relation to nonpublic personal information. (Copies of these "Principles of Support" are attached to this letter.) ACLI member companies have a long history of dealing with highly sensitive personal information, both medical and financial, in a professionally appropriate manner. We are proud of our record as custodians of this information.

We have also attached to this letter our detailed comments on each section of the proposed rule. We urge you to modify your final rule to take into account our suggestions and comments. We believe they raise important issues with regard to the ability of insurers to implement the rule in a manner that achieves the GLB Act's privacy goals while reducing the burden to consumers, customers and the financial services community.

At this point, we wish to highlight for your consideration a few of what we consider to be the more important issues. (For ease of presentation of a uniform submission to each of the agencies which have proposed privacy rules, the following generically references the relevant sections of your agency's rule.)

**§\_\_ .3(n), .3(o), and .3(p) Definitions of "nonpublic personal information," "personally identifiable financial information," and "publicly available information."**

The ACLI strongly believes that the definition of "publicly available information" should include any information *made available* to the general public (as provided in Alternative B of several of the agencies' proposals) as opposed to information which is *obtained from* public sources (as provided in Alternative A of several of the agencies' proposals). We do not believe that information which is available from public sources stops being public information simply because it is not obtained from public sources. Consumers have no expectation of privacy for information that is available from public sources. There is no benefit to consumers of requiring financial institutions to go to public sources to obtain information that is publicly available. A consumer's privacy is neither protected nor enhanced by

imposing such a burden on financial institutions. Accordingly, we strongly urge adoption of Alternative B with regard to the definitions of “nonpublic personal information” and “publicly available information.”

In addition, Section \_\_.3(o)(2)(C) of the proposed rule provides that the fact that an individual is or has been a customer of the financial institution is an example of “personally identifiable financial information.” We strongly object to this characterization. Customers do not regard the fact that they do business with a financial institution to be confidential. Indeed, every time a customer engages in a financial transaction with another person, the customer reveals the financial institution with which he or she does business. We do not believe that the fact that a customer has a continuing relationship with a financial institution should be regarded as “personally identifiable financial information.”

A list of customers therefore is derived using “publicly available information.” Consequently, a list comprised solely of customers’ names, addresses and telephone numbers should not be regarded as “nonpublic personal information.” A customer list of information that is otherwise publicly available, such as names, addresses and telephone numbers, cannot logically be regarded as “nonpublic” simply because it is presented in the form of a list. Accordingly, we urge you to confirm that a customer list is not “nonpublic personal information.”

The ACLI strongly objects to the fact that Section \_\_.3(o)(2)(i)(A) includes as an example of the definition of “personally identifiable financial information,” “information a consumer provides to you on an application to obtain...insurance..., including among other things, medical information.” As a result, all information collected in connection with a financial transaction is inappropriately swept into the definitions of both “personally identifiable financial information” and “nonpublic personal information.” This is in conflict with the provisions of the GLB Act, which are clear in limiting their protection to “financial” information.

Section 509(4) of Title V defines “nonpublic personal information” as “personally identifiable *financial* information” (emphasis added). Moreover, the fact that nonfinancial information is collected in connection with a financial transaction does not change the basic nature of the information itself. Finally, the Congress clearly did not intend for Title V to be applicable to medical information. It specifically declined to include a provision on the confidentiality of medical information.

The ACLI urges the agencies to narrow the scope of this example to *financial* information provided on an application. At a minimum, we urge deletion of the reference to medical information.

### **§§ \_\_.3(e) and .3(h) Definitions of “consumer” and “customer.”**

The definitions of “consumer,” set forth in Section \_\_.3(e) and “customer,” set forth in Section \_\_.3(h), give rise to particular and significant concerns as considered in the context of insurance. It is unclear whether the individual identified in these sections is the applicant, the policyholder, the insured (or certificateholder), or the beneficiary. However, it is essential for insurers to be able to identify the individuals to whom they are required to provide notices and the opportunity to opt-out.

During the application process, the insurer deals with the applicant. Once the policy is issued and coverage is effective, the insurer's contractual relationship is with the policyholder. The insurer may not have the address of an insured or the beneficiary. This is particularly true in the context of group insurance, where the insurer may not even have the names of the individuals insured. Accordingly, the ACLI urges that for purposes of individual and group insurance, the term "consumer" should, prior to the issuance of the policy, mean only the applicant. The term "customer" should mean only the policyholder.

#### **§\_\_\_.4 Initial notice to consumers of privacy policies and practices required.**

The proposed rule requires a financial institution to provide an initial notice to a consumer *prior to* the time the consumer establishes a customer relationship with the financial institution. We believe that this requirement is in conflict with the clear language of the GLB Act, which provides that a financial institution must provide the initial notice *at the time* of establishing a customer relationship. The proposed rule does not explain or justify why the agency is not following the clear and unambiguous terms of the GLB Act. We believe that often it will prove extremely difficult, if not impossible, for financial institutions to comply with a standard calling for provision of the initial notice *prior to* the time the customer relationship is established.

We urge you to amend this section to permit the initial notice to be provided *at or before* the time the customer relationship is established. This would resolve the conflict between the language of the GLB Act and the proposed rule. Most significantly, it would achieve the balance sought by the agencies in providing for the provision of initial notice at a meaningful time without unnecessarily burdening financial institutions. It would also allow for the flexibility necessary to accommodate the variety of business practices in today's fast changing financial services marketplace.

#### **§\_\_\_.5 Annual notices.**

The proposed rule states that notices must be provided annually to customers, and that "annually" means at least once during any period of twelve consecutive months during which the relationship exists. This permits a financial institution to provide an annual notice to all its customers at the same time each year. However, the language of the proposal could prove problematic in certain situations.

For example, a consumer becomes a customer on January 25, 2001, and receives an initial notice on that date. The financial institution sends annual notices to all customers on February 1, 2001. Under the proposed rule, the new customer may have to be sent another notice on February 1, 2001 in order to ensure that the customer receives the annual notice within 12 months. This result seems to impose an unreasonable burden on financial institutions (because it requires the financial institution to send far more disclosures than seems appropriate or desirable) without providing a corresponding consumer benefit. From the consumer's standpoint, he or she has already received the notice during that calendar year. Little, to no, purpose would seem to be served by requiring a financial institution to provide two notices during the calendar year in order to get all of its customers onto the same annual cycle.

Accordingly, we urge that the proposed rule be clarified to permit annual notices to be provided to customers at least once during each calendar year in which the relationship continues rather than during each 12 month period.

**§\_\_.6 Information to be included in initial and annual notices.**

The proposed rule provides that a financial institution must inform consumers of the categories of information that the institution collects and the categories of information that the institution discloses to third parties. However, the examples provided in connection with categories of information *collected* do not match the examples of the categories of nonpublic personal information the institution *discloses*. Examples given of the former include information such as application information and information about a deposit, loan or credit card account. Examples given of the latter are far more detailed, e.g., name, address, social security number, account balance and payment history.

We believe that the requirement of use of specific examples and the greater detail suggested for examples of categories of information disclosed is inappropriate. The GLB Act provides for the disclosure of *categories* of nonpublic personal information disclosed. The examples provided are not categories; they are the information disclosed. Accordingly, we urge you to amend the proposed examples of categories of information disclosed by using the same examples that are used in connection with the categories of information collected.

**§\_\_.12 Limitation on redisclosure and reuse of information.**

Sections \_\_.12(a)(2) and (b)(2) state that a financial institution or nonaffiliated third party which receives nonpublic personal information from a financial institution may only use the information for the purposes for which such information was provided. This is not consistent with the GLB Act.

First, Sections 504(a) and 505(a) of the GLB Act provide you with rulemaking and enforcement authority only over financial institutions normally subject to your enforcement authority under other law. There is no basis for extending the scope of the proposed rule to cover an entity that receives nonpublic personal information unless the recipient itself is a financial institution subject to your enforcement authority.

Second, Section 502(c) of the GLB Act provides that a nonaffiliated third party that receives nonpublic personal information from a financial institution shall not disclose such information to another person unless the disclosure would be lawful if made directly to the other person by the financial institution. Notwithstanding this clear language, the proposed rule provides limitations on the recipient of such information that go well beyond the GLB Act. There is no reason to impose further restrictions upon recipients since they are permitted by the GLB Act to disclose such information only to the extent the financial institution which had provided the information is permitted to disclose it.

There is also a practical problem with the approach proposed by the rule. A recipient may need to pass on the information it receives to a service provider, or it may need to use it for some other

operational reason which is unrelated to the purpose for which it received the information. Under the proposal, a receiver could not use the information to respond to a subpoena or to prevent or detect fraud unless the receiver had received it for those purposes. Accordingly, we request that the proposed rule reflect the provisions of the GLB Act, and permit the recipient of the information to use it for any permissible purpose.

**§\_\_.13 Limits on sharing of account number information for marketing purposes.**

You have asked whether there should be an exception to the prohibition on disclosing account numbers or access codes to nonaffiliated third parties for marketing purposes. The legislative history of the GLB Act indicates that financial institutions should be permitted to disclose customer account numbers or similar forms of access numbers or access codes in an encrypted, scrambled or similarly coded form if the consumer consents and the disclosure is necessary to process or service the transaction requested or authorized by the consumer. We strongly urge the agency to adopt an exception for the disclosure of account numbers with the consent of the individual.

We also believe that financial institutions should be permitted to disclose to nonaffiliated third parties encrypted, reference or truncated account numbers which are used for identification purposes. The prohibition in Section 502(d) of the GLB Act is intended to prevent potential abuse by limiting the ability of nonaffiliated third parties to make direct use of a consumer's account number. The use of an encrypted, reference or truncated account number to identify the consumer satisfactorily responds to the concerns which Section 502(d) was intended to address. It is important that nonaffiliated third parties be able to accurately identify customers by using unique numerical identifiers. Encrypted account numbers, reference numbers and truncated account numbers serve the purpose of providing a means of associating the consumer with a particular account without compromising the security and integrity of the consumer's account. Accordingly, we urge that the final rule adopt an exception which provides that the term "account number or similar form of access number or access code" does not include an encrypted account number, a reference number or a truncated account number which is provided to a nonaffiliated third party for use in marketing.

We also ask that you clarify the meaning of the term "transaction account" as used in Section \_\_.13. It is our understanding that the term transaction account means a "checking account," that is, an account which permits the consumer to make transfers or withdrawals by negotiable instrument or other device in order to make payments to third parties. We do not believe that it is intended to apply to an insurance policy or other type of insurance contract. The term transaction account is not generally used outside of the banking sphere, and will undoubtedly be confusing to financial institutions that are not banking institutions. We therefore believe it would be highly desirable for you to clarify the meaning of this term by referring to the term "transaction account" as used in Section 204.2(e) of Federal Reserve Regulation D, 12 C.F.R. Section 204.2(e).

**§\_\_ .16 Effective date and transition rule.**

The proposed rule indicates a scheduled effective date of November 13, 2000. We are very concerned that this will not provide the nation's more than 41,000 financial institutions with sufficient time in which to implement operational changes, reprogram computers, identify all of the sources and uses of consumer and customer information, prepare disclosure policies and train staff. It has been estimated that as many as two billion notices will be required to be sent to consumers and customers by November 13<sup>th</sup>. The scope and scale of the task is unprecedented, and it is highly unlikely that it can be successfully accomplished by November 13<sup>th</sup>. In order to provide an orderly transition, we strongly urge that the effective date be extended until November 12, 2001.

In the event the scheduled November 13, 2000 effective date is not extended, we are concerned that the proposed rule will in effect require that notices be provided by October 13<sup>th</sup> so as not to disrupt existing disclosure practices of financial institutions. The October 13<sup>th</sup> date reflects the latest date that notices can be sent to consumers and customers so that they will have an opportunity to opt out. Unless these notices are in the mail on October 13<sup>th</sup>, financial institutions will have to cease making disclosures to nonaffiliated third parties come November 13<sup>th</sup> until such time as consumers and customers have had a reasonable opportunity to opt out. This anomalous result is due to the initial timing for implementation of the GLB Act. Financial institutions will have a difficult enough time meeting the November 13<sup>th</sup> effective date. The agency should not impose an additional burden which would require heroic efforts to get disclosure notices in the mail to customers by October 13<sup>th</sup>. Accordingly, if the scheduled effective date is not changed, the proposed rule should be modified to permit a financial institution to continue to make disclosures of nonpublic personal information to nonaffiliated third parties for 30 days beginning November 13<sup>th</sup> unless the customer opts out before the 30 day period has run.

We appreciate the opportunity to comment on your proposed privacy rule.

Sincerely,



Roberta B. Meyer  
Senior Counsel  
on behalf of the  
American Council of Life Insurers

Enclosures

## 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.

**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.

**Detailed Comments of the American Council of Life Insurers  
on Proposed Privacy of Consumer Financial Information Rules<sup>1</sup>**

§ \_\_.1 Purpose and scope

Section \_\_.1(b) states that it applies to entities for which the agency has “primary supervisory authority.” Functional regulation established under the Gramm-Leach-Bliley Act (the “GLB Act”) vests supervisory authority over persons engaged in the business of insurance in the insurance authority of an insurer’s state of domicile. The ACLI requests that your rule affirm this principal of functional regulation.

§ \_\_.2 Rules of construction

The agencies have asked whether including examples in the proposed rules is useful. The ACLI believes that, provided they are not intended to provide the exclusive means of compliance, examples can be useful. However, we do have concerns with a number of the examples used in the proposed rules, as indicated below.

§ \_\_.3 Definitions

(a) Affiliate. No comment.

(b) Clear and Conspicuous. The ACLI believes that the proposed definition of the term itself is appropriate. ACLI member companies are committed to achieving effective, “clear and conspicuous”, communication of all the notices required under the GLB Act. However, the “examples” presented seem to be less examples than an exclusive set of rules indicating the manner in which a notice must be drafted in order to meet the “clear and conspicuous” requirement. Moreover, the fact that there appear to be three sets of rules, one providing how to make the notice “reasonably understandable” and two others providing how to design the notice “to call attention to its nature and significance,” is confusing.

All of the examples in Sections \_\_.3(b)(2)(i), (ii) and (iii) would seem to suggest ways in which the notice could be made reasonably understandable and designed to call attention to the nature and significance of the information contained in the notice. Accordingly, the ACLI suggests that the agencies amend Section \_\_.3(b)(2) to characterize all the examples provided in subsections (i), (ii), and (iii) as: “Examples of ways to make your notice clear and conspicuous.”

---

<sup>1</sup> For ease of presentation of a uniform submission to each of the agencies which have proposed privacy rules, the comment generically references the relevant sections of each agency’s rule.

- (c) Collect. No comment.
- (d) Company. No comment.
- (e) Consumer.- This definition, like that of “customer”, is problematic as applied in the context of insurance. Although the federal regulations generally do not directly govern actions taken in connection with the business of insurance, the ACLI raises this issue with the federal regulators because of its significance, the fact that the states are likely to use the federal rules as a template for any state rules to implement the GLB Act, and the critical need for consistency between the federal rules and any state rules that might be developed.

As applied in the context of insurance, this definition of “consumer” is ambiguous. It is unclear whether the individual identified is the applicant, the policyholder, the insured (or certificateholder), or the beneficiary. However, it is essential for insurers, like all financial institutions, to know the individual to whom they are required to provide notices and the opportunity to opt-out.

During the application process, the insurer deals primarily with the applicant. Subsequent to issuance of the policy, the insurer’s contractual relationship is with the policyholder. It is the policyholder who can exercise the rights of the insurance contract. The insurer is unlikely to have the address of an insured or beneficiary unless the insured or beneficiary is the same individual as the policyholder. This is particularly true in the context of group insurance, where the insurer may not even have the names of the individuals insured.

The ACLI urges the federal regulators to amend the definition of “consumer”, for purposes of individual and group insurance to mean, prior to issuance of the policy, only the applicant. (Upon issuance of the insurance policy, the consumer becomes a “customer.”)

- (f) Consumer reporting agency. No comment..
- (g) Control. No comment.
- (h) Customer. As discussed above, like the definition of “consumer”, this definition of the term “customer” is ambiguous as applied in the context of individual and group insurance. It is unclear whether it means the policyholder, the insured (or certificate holder), or the beneficiary. As noted above, after the policy is issued and coverage is in effect, the insurer’s contractual relationship is with the policyholder. Accordingly, the ACLI requests that the agencies amend this definition, for the purposes of both individual and group insurance, to mean only the policyholder.
- (i) Customer relationship. This definition is also ambiguous as applied in the context of insurance. The proposed rule is unclear as to when a “continuing relationship” begins in connection an insurance policy. Section \_\_.3(i)(2)(B)

provides that a consumer has a continuing relationship with the financial institution if the consumer “purchases an insurance product” from the financial institution. Again, it is unclear at what point a consumer “purchases” an insurance product.

Although the federal regulations are not directly applicable to insurers, for the reasons noted above in relation to the definitions of “consumer” and “customer,” the ACLI believes it important for the federal regulators to clarify this definition as it relates to insurers. The ACLI strongly urges that the example set forth at Section \_\_.3(i)(2)(B) make it clear that the consumer has a continuing relationship when the policy is issued and insurance coverage is in effect. This will provide needed specificity with regard to the person with whom the insurer has a customer relationship and the time at which that relationship begins.

- (j) Financial institution. The intent of Title V of the GLB Act is to govern the information sharing practices of financial institutions. As defined in Section 509(3) of the GLB Act a financial institution is “...any *institution* the business of which is engaging in financial activities...” (emphasis added). However, the definition of financial institution should make it clear that a sole proprietorship is not a financial institution under the GLB Act.

Moreover, many insurance agents and other providers of financial services, for financial reasons, have chosen to operate as sole proprietorships rather than assume another business organizational form. Because they are generally small, sole proprietorships would find it enormously burdensome to comply with the requirements of the GLB Act and the proposed rules. There would be questionable corresponding benefit to consumers who would still be provided the requisite notices and the opportunity to opt-out by the insurers with which the agent sole proprietor is doing business. For these reasons, the ACLI requests that the agencies amend this definition to clarify that it does not include a sole proprietorship.

- (k) Financial product or service. The ACLI strongly objects to this broadening of the usual and customary definition of the term “financial service” by including within its scope the evaluation of information submitted under an application. Section \_\_.3(k)(2). We question whether it is within the agencies’ statutory authority under the GLB Act to broaden the definition of this term in this manner and whether it will benefit consumers in any way. We understand the possible concern that information contained on applications could potentially be disclosed to nonaffiliated third parties. However, we do not believe that the language nor the intent of the GLB Act reaches the application process. Accordingly, we object to the agency’s attempt to expand the usual and customary definition of the term “service” to cover an evaluation of an application.
- (l) Government regulator. The legal significance of the qualification to the reference to a state insurance authority, “with respect to any person domiciled

in that insurance authority's State that is engaged in providing insurance," is unclear. This is not the approach taken with regard to the other agencies specified in the definition. None of the references to any of the federal regulators are qualified. Therefore, the ACLI requests that Section \_\_.(3)(1)(8) should be amended to strike the qualifying language and to read "A State insurance authority;"

- (m) Nonaffiliated third party. The ACLI strongly objects to the language of this definition that would include within its scope companies which represent downstream investments of insurers. This will cause these companies to be excluded from the scope of the definition of "affiliate" in Section 509(6) of the GLB Act and Section \_\_.3(a) of the proposed rule, which include any company which is "controlled by" a financial institution. There would appear to be neither a legal basis nor anticipated consumer benefit for excluding such companies in this manner from the scope of the term "affiliate."

The practical effect of the definition will be to preclude any company controlled by an insurance company from being regarded as an affiliate of an insurer because insurance companies do not as a practical matter distinguish between the different legal authorities used to make certain types of investments. This definition will impose a particular hardship on insurance companies that are not part of financial holding companies, for they have no reason to distinguish between financial activities and other activities engaged in by companies in which they invest.

- (n) Nonpublic personal information. The ACLI strongly supports Alternative B which is discussed in the Supplementary Information to the agency's proposed rule. The ACLI believes that the definition of "publicly available information" should include information *made available* to the general public as opposed to information made available to the general public that is *obtained from* public sources.

We do not believe that information which is available from public sources stops being public information simply because it is obtained from a consumer rather than from public sources. We question the benefit to consumers of requiring financial institutions to go to public sources to ensure that the information is publicly available.

A list of customers is derived using "publicly available information," and consequently is not "nonpublic personal information." An individual's status as a customer of a particular financial institution is ordinarily public information. Any time a consumer uses a personal check or credit card, he or she identifies and makes public the financial institution with which he or she is doing business. There is no expectation among consumers that, under such circumstances, their status as customers of specific financial institutions will be regarded as private.

The ACLI strongly urges adoption of Alternative B with respect to the definitions of “nonpublic personal information” and “publicly available information.” We also urge deletion of the example provided at Section \_\_.3(n)(3), which provides that “nonpublic personal information includes any list of individuals’ street addresses and telephone numbers that is derived using personally identifiable financial information, such as account numbers.”

The Supplementary Information specifically invites comment “on whether either definition of ‘nonpublic personal information’ would cover information about a consumer that contains no indicators of a consumer’s identity.” Section 509(4)(A) of the GLB Act clearly provides that the “term ‘nonpublic personal information’ means *personally identifiable* financial information...” (emphasis added). Therefore, if consumer information does not contain indicators of the consumer’s identity, then it fails to meet one of the two core requirements of the statutory definition of “nonpublic personal information” – the fact that it must be personally identifiable, as well as financial information. This is true regardless of the breadth of the definition of “publicly available information.”

Consequently, neither alternative definition of “nonpublic personal information” would include information about a consumer that has no identifiers. The ACLI urges the agencies to amend the definition of “nonpublic personal information” to clarify this point.

- (o) Personally identifiable financial information. The ACLI is concerned by the inappropriate breadth of the term “personally identifiable financial information” which is contained in the proposed rule.

#### Fact that Individual is or has been a Customer

The ACLI strongly objects to the example provided at Section \_\_.3(o)(2)(i)(C), which treats as “personally identifiable financial information” the fact that a person is a customer of the financial institution. We believe that this result is not in accord with the definition of the term “nonpublic personal information” in Section 509(4) of the GLB Act, because customer status is not “financial” information.

Moreover, a customer list does not provide any information about a consumer that should be considered “nonpublic personal information”. As noted above in our discussion of the definition of “nonpublic personal information,” an individual’s status as a customer of a particular financial institution is ordinarily public information. Consumers do not expect that their status as customers of specific financial institutions will be kept private. Accordingly, the ACLI urges that the example set forth at Section \_\_.3(o)(2)(i)(C) be deleted.

#### Medical and Other Nonfinancial Information

The ACLI strongly objects to the fact that the definition of “personally identifiable financial information” includes as an example “information a consumer provides to you on an application to obtain...insurance..., including among other things, medical information.” (Section 3(o)(2)(i)(A)). As a result, all information collected in connection with a financial transaction is inappropriately swept into the definitions of both “personally identifiable financial information” and “nonpublic personal information.” This is in conflict with the provisions of the GLB Act, which are clear in limiting their protection to “financial information.”

As noted above, the definition of “nonpublic personal information” in Section 509(4) of the GLB Act provides that information must be *financial*, as well as personally identifiable, to meet the core requirements of the definition. The fact that nonfinancial information is collected in connection with a financial transaction does not change the basic nature of the information itself. Moreover, the Congress clearly intended that the provisions of the GLB Act not be applicable to medical information. During the course of consideration of the GLB Act, Congress specifically rejected a provision subjecting medical information to the provisions of the legislation.

Moreover, medical information is generally viewed as different from and much more sensitive than financial information. The recent adoption of the National Association of Insurance Commissioners (NAIC) Health Information Privacy Model, which deals exclusively with the confidentiality of medical information, is a reflection of the NAIC’s appreciation of the need to treat the confidentiality of medical information separate from that of financial information. Similarly, the ACLI has adopted a separate policy on the confidentiality of medical information which is different from our policy on the confidentiality of financial information. Our medical information policy reflects our member companies’ view that medical information should be afforded special treatment. It includes support of a legislative or regulatory prohibition on the sharing of medical information for marketing purposes.

In addition, as the agency noted in the Supplementary Information, there “...are other laws that may impose limitations on disclosure of nonpublic personal information in addition to those imposed by the G-L-B Act and these rules.” This is particularly true with respect to the confidentiality of medical information. The inclusion of medical information in the definitions of “personally identifiable financial information” and “nonpublic personal information” would impose requirements in relation to the sharing of medical information that are inconsistent, if not in conflict, with the limitations and requirements of many of the existing federal and state confidentiality laws as well as the proposed Department of Health and Human Services regulations to implement the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This will create much confusion as to insurers’ confidentiality obligations.

In view of the above, the ACLI strongly encourages the agencies to narrow the scope of the example of “personally identifiable financial information”, provided at Section \_\_.3(o)(2)(i)(A), to *financial* information provided to obtain insurance and other financial products or services. At a minimum, we strongly urge deletion of the reference to medical information.

- (p) Publicly available information. As noted above, the ACLI urges the agencies to adopt the definition of “publicly available information” set forth in Alternative B, which treats information as publicly available if it is *made available* to the general public from public sources.

Also, the ACLI believes that the definition of the term “publicly available information” is unreasonably narrow because it unreasonably limits the sources from which publicly available information may be obtained to government records, the media, and disclosures required by law. Information should be able to qualify as publicly available information so long as it is made available from public sources. The ACLI urges the agencies to amend this definition accordingly.

- (q) You. No comment.

#### § \_\_.4 Initial notice to consumers

The ACLI strongly opposes the requirement contained in \_\_.4(a)(1) that initial privacy notices be provided *prior to the time* the financial institution establishes a customer relationship. By contrast, Section 503 of the GLB Act provides that an initial disclosure must be made *at the time of* establishing a customer relationship with a consumer. The Supplementary Information to the proposed rule notes that the proposed rule’s “approach is intended to strike a balance between: (1) Ensuring that consumers will receive privacy notices at a meaningful point along the continuum of establishing a customer relationship; and (2) minimizing unnecessary burdens on financial institutions that may result if a financial institution is required to provide a consumer with a series of notices at different times in a transaction.”

We believe that the “prior to” requirement the agency has proposed is contrary to the GLB Act and will prove difficult and overly burdensome to meet. It will require financial institutions to first determine when the customer relationship is established, and then just before that time, provide the required notice to the customer. This approach is inconsistent with normal business practices. It also fails to allow for the flexibility necessary to accommodate the variety of business practices in today’s rapidly changing financial services market. It will impose burdens on financial institutions which are not needed to ensure that the consumer will receive privacy notices at a meaningful time.

The ACLI strongly urges the agencies to amend Section \_\_.4(a)(1) to permit the initial notice to be provided “*at or before*” the time the customer relationship is

established. This would conform the language of the proposed rule to that of the GLB Act.

The Supplementary Information indicates that affiliated financial institutions may use a common notice. We believe that this is an important point and should be incorporated into the rule.

#### § \_\_.5 Annual notice to customers

Section 503(a) of the GLB Act requires that privacy notices be provided at the time a customer relationship is established and no less frequently than annually during the continuation of the relationship. The proposed rule provides that a notice must be sent to customers at least once during any 12 month period during which the relationship exists. The ACLI believes that the requirement of providing notice “once every 12 month period” is problematic.

If the proposed rule is unchanged, a financial institution which desires to send the required annual mailing to all of its customers on the same date would have to send many more notices than would seem desirable or intended by the GLB Act or the proposed rule. The financial institution would incur substantial additional costs in order to achieve this result.

For example, a consumer becomes a customer on January 25, 2001, and receives an initial notice on that date. The financial institution sends annual notices to all customers on February 1, 2001. Under the proposed rule, the new customer may have to be sent another notice on February 1, 2001 in order to ensure that the customer receives the annual notice within 12 months. This result seems to impose an unreasonable burden on the financial institution (because it requires the financial institution to send far more disclosures than seems appropriate) without providing a corresponding consumer benefit. From the consumer’s standpoint, he or she has already received the notice during that calendar year. Little, to no, purpose would seem to be served by requiring the financial institution to provide two notices during the calendar year in order to get all of its customers onto the same annual cycle.

To avoid this needless burden, the ACLI urges that the proposed rule be clarified to permit financial institutions to have the flexibility to send customers annual notices at least once during each calendar year, beginning immediately after the customer establishes a relationship with the financial institution. For example, a financial institution would be required to send an initial notice to a customer at the time the relationship is established. In subsequent calendar years, the financial institution would be required to send the annual notice to the customer before December 31<sup>st</sup>. This approach would result in considerable savings for financial institutions because it would enable them to send notices once each calendar year to all customers in one mailing. Such an approach is consistent with the GLB Act because each customer would in fact receive a notice annually.

## § \_\_.6 Information to be included in initial and annual notices

The ACLI agrees with the agency that the same information should be provided in both the initial and annual notices. We also believe that it is appropriate to require the notices to list the *categories* of information that may be collected, such as application information, transaction information and consumer report information.

While we believe it is also appropriate that the notice be required to list the *categories* of nonpublic personal information that the financial institution discloses, we do not believe that requiring financial institutions to provide *examples* of the categories of information disclosed is appropriate. Section \_\_.6(d)(2). We believe the examples of the categories of information provided in the proposed rule with respect to “disclosures” should match the examples of the categories of information provided in the proposed rule with respect to “information collected.” Requiring a financial institution to provide specific examples of the information which may be disclosed, rather than categories of information to be disclosed, will be confusing to customers and unnecessarily burdensome to financial institutions. The ACLI urges the agencies to amend the example set forth at Section \_\_.6(d)(2) to make the examples of categories of information disclosed the same as the examples of the categories of information collected, and to delete the requirement of providing specific examples of information to be disclosed.

In response to the request for comments in the Supplementary Information, the ACLI believes that a financial institution that uses a third party to perform services for the institution need not disclose this to customers if the transaction comes within one of the exceptions provided in § 502(e) of the GLB Act. Under section \_\_.6(b), the financial institution must inform consumers that it makes disclosures as permitted by law to nonaffiliated third parties in addition to those described in the notice. We believe that this notice is adequate under the GLB Act.

The ACLI urges the agencies to adopt standards under § 501 of the GLB Act relating to administrative, technical and physical safeguards as soon as possible in order to provide guidance to financial institutions as to what types of disclosures will be acceptable.

## § \_\_.7 Limitation of disclosure to nonaffiliated third parties

The proposed rule states that a financial institution may not disclose nonpublic personal information to a nonaffiliated third party unless the consumer has been given an opportunity to opt out from such disclosure. We believe that the rule should not provide examples of the time periods during which the consumer has an opportunity to opt out. Rather, the time periods should depend upon the specific facts and circumstances involved.

Further, the ACLI believes that financial institutions should not be required to send multiple opt out notices to customers who maintain joint accounts. Rather, it is appropriate to send one notice and opportunity to opt out to the address indicated in the institution's records.

#### § \_\_.8 Form and method of providing opt out notice

The Supplementary Information to the proposed rule states that a financial institution is not required to provide an opt out notice when a customer establishes a new type of customer relationship. This section, however, does not appear to include this important provision. We recommend that this point be included in the language of the final rule.

The ACLI believes that the agency should make it clear that the examples provided in \_\_.8(a)(2) are not exclusive, but merely illustrative of the ways in which a financial institution may provide consumers with an opportunity to opt out.

The ACLI also believes that a financial institution should be required to provide a notice of change in terms to consumers before being permitted to disclose nonpublic personal information only if the change in terms is material or substantial. We believe that a financial institution should not be required to send a new notice to its customers if changes to its privacy policies are minor or insignificant.

The proposed rule states that a consumer's revocation of his or her decision to opt out must be in writing or in electronic form. We believe that this is overly burdensome and could prove detrimental to consumers. Consumers should have the opportunity to revoke their opt outs orally. We believe this could prove beneficial to customers in that it enables financial institution to contact customers by telephone and receive their consent to a disclosure that would enable information to be disclosed to a nonaffiliated third party to explain a new product or service to the customer. Institutions would undoubtedly retain records to ensure that the revocations were valid. A requirement of written revocation would be burdensome and contrary to the consumer's interests. Accordingly, we believe Section \_\_.8(e) should be amended to permit a consumer to revoke an opt out orally if followed by a written confirmation by the financial institution.

#### § \_\_.9 Service provider and joint marketing exceptions

Section \_\_.9(a)(2)(ii) permits information which is disclosed to a third party in accordance with this exception to be used only for the purposes for which the information is disclosed or in accordance with the processing or other listed exceptions. The GLB Act does not limit subsequent disclosures by third parties in this manner. Section 502(b)(2) of the GLB Act provides that the third party need only agree to maintain the confidentiality of the information. As indicated in § 502(c) of the GLB Act, a third party that receives nonpublic personal information under section 502 may not disclose such information to a

nonaffiliated third party of both the financial institution and the third party unless such disclosure would be lawful if made directly to the other person by the financial institution.

The restriction in the proposed rule goes beyond the scope of that provided in the Act. Congress did not intend to limit the use of information obtained by third parties solely to the purpose for which it was provided. If the financial institution could lawfully disclose the information, there is no reason why a third party should be so limited. The ACLI urges the agency to conform the proposed rule to the provisions of the GLB Act.

The issue has been raised as to whether to require financial institutions to take steps to assure that the product being jointly marketed and the other participants in the joint marketing agreement do not present undue risks for the institution. The ACLI does not believe it is appropriate to impose such requirements on financial institutions under this rule. Such requirements should be considered in the context of laws which directly address the safety and soundness of financial institutions.

#### § \_\_.10 Exceptions for processing and servicing.

The ACLI believes that the exceptions provided in Section \_\_.10 generally follow Section 502(e) of the GLB Act. We suggest that the structure of the GLB Act be preserved. The words “in connection with” which appear in Section 502(e)(1) should modify Section \_\_.10(a)(2), (3) and (4), as they do in the GLB Act. Section \_\_.10(a)(1) of the proposed rule deletes the words “or in connection with” which are contained in the GLB Act. We believe that this is an important deviation, for Congress intended the processing exception to apply “as necessary to effect, administer or enforce a transaction requested or authorized by the consumer,” “or in connection with servicing or processing a financial product or service requested or authorized by the consumer.” This latter clause may not relate to a transaction requested or authorized by the consumer despite the fact that the product or service was requested or authorized by the consumer. Unless this exception is included as provided for in the GLB Act, we are concerned that a gap may exist which could interfere with the efficient delivery of products and services to consumers.

A similar concern exists with regard to the exceptions for maintaining or servicing a customer’s account for securitizations which appear in Section \_\_.10(a)(3) and (4). We urge that the language of the statute be reflected in this section of the rule.

#### § \_\_.11 Other exceptions

Under the proposed rule, a consumer may consent to the disclosure of information by the financial institution. The agency has asked whether a financial institution should require a consumer to provide such consent in writing. For the

reasons presented above with regard to a consumer's ability to orally revoke his or her opt out, we believe that a consumer's consent should be permitted to be made in any manner, including orally.

#### § \_\_.12 Limits on redisclosure

Sections \_\_.12(a)(2) and (b)(2) state that a financial institution or nonaffiliated third party which receives nonpublic personal information from a financial institution may only use the information for the purposes for which such information was provided. This is not consistent with the GLB Act.

Sections 504(a) and 505(a) of the GLB Act provide the agency with rulemaking and enforcement authority only over financial institutions normally subject to the agency's enforcement authority under other law. There is no basis for extending the scope of the rule to cover an entity that receives nonpublic personal information unless the recipient itself is a financial institution subject to the agency's enforcement authority.

Section 502(c) of the GLB Act provides that a nonaffiliated third party that receives nonpublic personal information from a financial institution shall not disclose such information to another person unless the disclosure would be lawful if made directly to the other person by the financial institution. Notwithstanding this clear language, the proposed rule imposes limitations on the recipient of such information that go well beyond the GLB Act. There is no reason to impose further restrictions upon recipients since they are permitted by the GLB Act to disclose such information only to the extent the financial institution which had provided the information is permitted to disclose it.

There is also a practical problem with the approach of the proposed rule. A recipient may need to pass on the information it receives to a service provider, or it may need to use it for some other operational reason which is unrelated to the purpose for which it received the information. Under the proposal, a receiver could not use the information to respond to a subpoena or to prevent or detect fraud unless the receiver had received it for those purposes. Accordingly, we request that the proposed rule reflect the provisions of the GLB Act, and permit the recipient of the information to use it for any permissible purpose.

#### § \_\_.13 Limits on sharing account number information

The agency has asked whether there should be an exception to the prohibition on disclosing account numbers or access codes to nonaffiliated third parties for marketing purposes. The legislative history of the GLB Act indicates that financial institutions should be permitted to disclose customer account numbers or similar form of access numbers or access codes in an encrypted, scrambled or similarly code form if the consumer consents and the disclosure is necessary to process or service the transaction requested or authorized by the consumer. We strongly urge the agency to adopt exceptions for the disclosure of account numbers with the consent of the individual.

We also believe that financial institutions should be permitted to disclose to nonaffiliated third parties encrypted, reference or truncated account numbers which are used for identification purposes. The prohibition in Section 502(d) of the GLB Act is intended to prevent potential abuse by limiting the ability of nonaffiliated third parties to make direct use of a consumer's account number. The use of an encrypted, reference or truncated account numbers to identify the consumer satisfactorily responds to the concerns which Section 502(d) was intended to address.

It is important that nonaffiliated third parties be able to accurately identify customers to the financial institution by using unique numerical identifiers. Encrypted account numbers, reference numbers and truncated account numbers serve the purpose of providing a means of associating the consumer with a particular account without compromising the security and integrity of the consumer's account. Accordingly, we urge that the final rule adopt an exception which provides that the term "account number or similar form of access number or access code" does not include an encrypted account number, a reference number or a truncated account number which is provided to a nonaffiliated third party for use in marketing.

We also ask that you clarify the meaning of the term "transaction account" as used in Section \_\_.13. It is our understanding that the term transaction account means a "checking account," that is, an account which permits the consumer to make transfers or withdrawals by negotiable instrument or other device in order to make payments to third parties. We do not believe that it is intended to apply to an insurance policy or other type of insurance contract. The term transaction account is not generally used outside of the banking sphere, and will undoubtedly be confusing to financial institutions that are not banking institutions. We therefore believe it would be highly desirable for you to clarify the meaning of this term by referring to the term "transaction account" as used in Section 204.2(e) of Federal Reserve Regulation D, 12 C.F.R. Section 204.2(e).

#### § \_\_.14 Protection of the Fair Credit Reporting Act

The ACLI strongly supports the agency's proposed rule that reaffirms that the rule does not affect the Fair Credit Reporting Act.

#### § \_\_.15 Relation to State laws

This provision restates Section 507 of the GLB Act. However, the GLB Act grants authority to the Federal Trade Commission ("FTC") to make the determination as to whether a State law is inconsistent with the provisions of the *GLB Act*. Section 507 does not grant the FTC authority to make a determination concerning the inconsistency of a State law with the rule of an agency. We do not believe the FTC possesses such authority. Accordingly, we believe Section \_\_.15(b) should be deleted.

§ \_\_.16 Effective date

The proposed rule indicates a scheduled effective date of November 13, 2000. We are very concerned that this will not provide the nation's more than 41,000 financial institutions with sufficient time in which to implement operational changes, reprogram computers, identify all of the sources and uses of consumer and customer information, prepare disclosure policies and train staff. It has been estimated that as many as two billion notices will be required to be sent to consumers and customers by November 13<sup>th</sup>. The scope and scale of the task is unprecedented. It is highly unlikely that it can be successfully accomplished by November 13<sup>th</sup>. In order to provide an orderly transition, we strongly urge that the effective date be extended until November 12, 2001.

In the event the scheduled November 13, 2000 effective date is not extended, we are concerned that the proposed rule will in effect require that notices be provided by October 13<sup>th</sup> so as not to disrupt existing disclosure practices of financial institutions. The October 13<sup>th</sup> date reflects the latest date that notices can be sent to consumers and customers so that they will have an opportunity to opt out. Unless these notices are in the mail on October 13<sup>th</sup>, financial institutions will have to cease making disclosures to nonaffiliated third parties come November 13<sup>th</sup> until such time as consumers and customers have had a reasonable opportunity to opt out. This anomalous result is due to the initial timing for implementation of the GLB Act. Financial institutions will have a difficult enough time meeting the November 13<sup>th</sup> effective date. The agency should not impose an additional burden which would require heroic efforts to get disclosure notices in the mail to customers by October 13<sup>th</sup>. Accordingly, if the scheduled effective date is not changed, the ACLI urges that the proposed rule be modified to permit a financial institution to continue to make disclosures of nonpublic personal information to nonaffiliated third parties for 30 days beginning November 13<sup>th</sup> unless the customer opts out before the 30 day period has run.