42

May 1, 2002

Regulations and Legislative Division
Chief Counsel's Office
Office of Thrift Supervision
1700 G. Street
Washington, D.C. 20552

Attn: Study on GLBA Information Sharing

Re: Comments on the GLBA Information Sharing Study

Dear Chief Counsel:

On behalf of the National Association of Mutual Insurance Companies ("NAMIC"), we respectfully submit the comments below for purposes of the interagency study regarding information sharing under the Gramm-Leach-Bliley Act ("GLBA") announced in the *Federal Register* on February 15, 2002.[1]

NAMIC is a full-service international trade association with more than 1,200 member companies that underwrite 40 percent ($123.3 billion) of the property/casualty insurance premiums in the United States. NAMIC's membership ranges from multinational insurers to single-county insurers. Our members include five of the ten largest U.S.-based property/casualty carriers, every size regional and national property/casualty insurer and hundreds of farm mutual insurance companies. Many of our member companies are affiliates of other financial institutions, including affiliated insurers. Some member companies have financial service operations that include banking or securities investment products in addition to the more typical mutual insurance multi-lines offered through insurance affiliates.

NAMIC's mutual insurance company members are owned by their policyholders. The mutual ownership structure imposes on the insurer unique obligations to serve customer needs. These needs may vary by institution and individual customer, but regardless of the size of company, number of affiliates, or variety of financial or insurance products and services provided, the customers of our member companies have a common, fundamental expectation: that their chosen company and its affiliates know them and will provide them with appropriate advice based on that knowledge. Meeting

---

[1] 67 Fed. Reg. 7,213 (Feb. 15, 2002).

this fundamental expectation necessarily requires sharing of customer information with both affiliates and nonaffiliated third parties, as discussed below.

NAMIC member company customers, like those of other financial institutions, also have data privacy expectations and interests. We respect those interests, which we believe are well protected by the existing privacy regulations under both the GLBA and the federal Fair Credit Reporting Act ("FCRA"), as well as the medical information privacy standards promulgated by the Department of Health and Human Services ("HHS"). In light of these existing, relatively new and very comprehensive sets of regulations, we strongly oppose additional privacy legislation or regulation governing financial institutions' information sharing at either the federal or state level, at least at this time.

1. Purposes of Sharing Confidential Customer Information With Affiliates or With Nonaffiliated Third Parties

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

NAMIC member companies share a variety of types of customer information with their affiliates, most of which is basic data obtained through the customer application. Typically, this includes name, address, and certain background and prior insurance information. Unique identifiers for individuals are particularly important to be shared, in order to ensure accuracy in servicing each individual customer appropriately.

Payment history and claim history are also examples of customer information that may be shared among affiliates. Reasons for such sharing range from providing consolidated billing among affiliated companies to addressing patterns of claims that may prompt an insurer to recommend a different deductible.

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

The principal types of information shared by NAMIC member companies with nonaffiliated third parties are those types of data, including name, address and insurance coverage information, that are needed for third parties to assist in the process of underwriting insurance applicants and adjusting the claims of current policyholders. For example, our member companies share customer information with auto repair shops to assist in the resolution of an auto damage claim. The provision of basic personal

identification and scope of insurance coverage information provides such nonaffiliated third parties with the contact and related data without which it would be impossible to resolve a customer claim or provide another type of service integral to the insurance process.

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 nonaffiliated third parties.***

In general, NAMIC member companies share the same basic types of customer identification and insurance coverage information with affiliated and with nonaffiliated third parties. However, information is shared only on a "need-to-know" basis, so only such information as is required to permit the affiliate or nonaffiliated third party to perform the function requiring customer data is actually shared. In general, this results in sharing less information with nonaffiliated third parties than with affiliated companies. For example, information may be shared with affiliates for marketing purposes while this would be done with nonaffiliated third parties only under limited circumstances.

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

Our member companies share customer information with affiliates for a range of key insurance purposes, including underwriting, claim handling, rating, identification and a number of administrative functions, such as billing and agent information. In addition, our member companies share customer information with their affiliates to ensure that the customer, in purchasing an insurance or other financial product from an affiliated company, will be properly familiar to the affiliate with whom he or she is transacting business. This enables our member companies to provide their customers the appropriate service and to advise them about suitable products and services available to them through affiliated companies.

Many of our member companies interact with their customers through agents. Some maintain agents on an exclusive basis; others on a producer-independent agent basis, where the agent of record has access to and contracts or appointments with more than one insurance carrier or insurance group. In many instances, our member companies may share a common data processing or information system for information collected by agents, so that basic customer information is accessible to company affiliates through a central database. Other member companies that do not function through agents also may

maintain such shared databases. In either case, the shared data system permits companies within a single affiliated group to provide billing information, keep track of where the customer resides, and monitor the financial product needs of the customers or joint policyholders in a manner that avoids inaccuracies, duplication, inefficiency and excess cost.

Another purpose for which our member companies share customer information with affiliates is to identify the affiliates' experience with the customer for underwriting and rating purposes. For example, in many of our member companies, a discount is provided for purchase of multi-line insurance products. In order to provide a customer with this discount, the fact that the customer purchased, for example, home insurance from one affiliate and car insurance from another would need to be shared between the two affiliated companies. Such "relationship pricing" is among the key benefits to NAMIC member company customers from affiliate information sharing, as discussed further in section 5 below.

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

As noted above in response to question 1(b), a key purpose for which NAMIC member companies share customer information with nonaffiliated third parties is to enable those third parties to assist in insurance underwriting and claims processing. Some of our member companies contract with outside claim handlers and share customer information in the normal course of handling a claim. Others use third parties for data processing. In rating, underwriting, and claim adjustments, an insurer may quite literally be contracting with more than tens of thousands of third parties to accomplish ordinary customer service functions. Many companies control costs, and ultimately premiums, by contracting with these third parties for the provision of specific services. The third party, such as claim adjuster, can generally provide the service at a lower cost than would be involved in the company performing the service "in house." Such cost-savings are important for all companies, and may be critical for medium and smaller-size insurers. Laws or regulations that limit these relationships may be damaging to the insurance industry.

NAMIC member companies share customer information with nonaffiliated third parties not only for fundamental insurance purposes such as claim handling and underwriting, but also to protect themselves and their customers against fraudulent or otherwise unauthorized transactions. This latter purpose is critically important to protect

policyholders from the significant costs that insurance fraud and material misrepresentation imposes on insurers.

According to a recent report by the Insurance Information Institute,[2] property/casualty insurance fraud costs insurers about $30 billion annually. Fraud may be committed at different points in the insurance transaction by many individuals: applicants for insurance, policyholders, third-party claimants and professionals who provide services to claimants. Common automobile and homeowner's insurance frauds include misrepresenting facts on an insurance application; submitting claims for injuries or damage that never occurred; "staging" accidents; and "padding," or inflating actual claims.

Workers' compensation insurance fraud is also a serious problem. For example, employers, seeking to obtain a lower premium, may misrepresent their payroll or the type of work carried out by their employees. These two factors are important in calculating workers' compensation insurance premiums because they represent the potential for claims. Medical care abuse is another element of workers' compensation fraud: health care providers frequently "upcode" – exaggerate – the treatment provided. Claimants may also abuse the system by over-utilizing medical care to keep receiving indemnity benefits.

Many insurance companies have established special investigation units ("SIUs") to help identify and investigate suspicious claims. Some insurance companies outsource their SIUs to other insurers. SIUs range from a small team whose primary role is to train claim representatives to deal with the more routine kinds of fraud cases to teams of trained investigators, including former law enforcement officers, attorneys, accountants and claim experts to conduct thorough investigations. More complex cases, involving large-scale criminal operations or individuals that repeatedly stage accidents, may be turned over to the National Insurance Crime Bureau ("NICB"). This insurance industry-sponsored organization has special expertise in preparing fraud cases for trial and serves as a liaison between the insurance industry and law enforcement agencies. In addition, it publicizes the arrest and conviction of the perpetrators of insurance fraud to help deter future criminal activities.

---

2 Insurance Information Institute, "Hot Topics and Insurance Issues" (March 2002).

Recently, the threat of insurance fraud has taken on new dimensions in light of concern that ill-gotten gains reaped by organized fraud rings have been used to fund terrorism. In order for insurers to pursue or assist in the prosecution of fraud, they must be able to share information on individuals suspected of wrongdoing. Privacy laws that inhibit such information sharing pose an obstacle to fraud detection, investigation, and reduction. Although most current privacy laws contain exceptions to permit information sharing for antifraud purposes, some do so on a very limited basis. These laws may thereby be harming the very individuals they are designed to protect. There is no question that insurance fraud raises policyholder premiums. It is critical for all insurance customers, therefore, that data privacy laws not prevent insurers from sharing customer information with nonaffiliated third parties to assist in antifraud efforts.

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

Many of our member companies have an established business practice not to sell any customer information. Others do not provide customer information to any person or organization outside their affiliated companies for the marketing purposes of these nonaffiliated third parties. Many, if not most, of our member companies do not share customer medical information (which they may receive as a consequence of claims under an automobile or homeowner's insurance policy) unless expressly authorized to do so by the customer. Many companies will not share customer information, even where permitted by law, unless such disclosure is *required* under process of law by a subpoena or other legal compulsion.

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

For affiliated companies, the most obvious operational limitation on information sharing is systems configurations. Systems configurations may also impose some limits on data sharing with nonaffiliated third parties. In addition, there are contractual limits on data sharing by insurers with certain nonaffiliated third parties, such as the Insurance Services Office, which consolidates insurance experience data for rating purposes. Property/casualty companies and corresponding servicing third-party entities and life insurance companies and their servicing entities also adhere to traditionally established limits in sharing certain types of customer information to ensure proper customer and company confidentiality. For example, it is an established rule that the Medical

Information Bureau, which maintains a database of medical claims information for fraud detection purposes, does not share information with a property/casualty insurance carrier.

h. ***For what other purposes would financial institutions like to share information but currently do not? What benefits would financial institutions derive from sharing information for those purposes? What currently prevents or inhibits such sharing of information?***

Our member companies would like to be able to more freely share non-transaction/experience information among affiliated companies. Although we believe the FCRA opt-out requirements with respect to information sharing with affiliates are reasonable in principle, we also believe our member companies' customers would benefit from the reduced costs that would be possible if the FCRA opt-out requirement applied to a narrower scope of information. For affiliated insurers, the FCRA opt-out requirement frequently imposes a non-consumer-friendly limitation on sharing of information derived in the application process. For example, information obtained from a consumer's application for insurance from an automobile or homeowners insurance carrier, if shared with an affiliated carrier with whom the customer already has coverage, can benefit the applicant by enabling the new policy to be provided based on discounted rates. The costs entailed in administering an opt-out procedure within the insurance affiliate structure for this type of information are high relative to any possible consumer benefit.

We also note that certain state laws, such as those of Vermont, restrict information sharing with affiliates and/or nonaffiliated third parties in ways that are inconsistent with the fundamental goals of both the GLBA and the FCRA. Our member companies believe that such state laws are a serious impediment to servicing their insurance customers and that a uniform information-sharing standard is needed to prevent the inevitable costs of inconsistent standards on financial institutions and their customers. The need for providing such uniformity is particularly critical in light of the rapid expansion of business through the Internet and cyberspace.

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

a. ***Describe the kinds of safeguards that financial institutions have in place to protect the security of information.***

NAMIC member companies maintain a wide variety of physical, electronic and organizational safeguards to protect customer information. Some companies use encrypted software; some limit access to electronic data by requiring passwords and special log-on identification terms. Others protect data stored in hard copy by employee identification card or badge requirements. Our member companies generally review on an ongoing basis their information security policies and practices, regularly monitor their computer networks, and frequently test the strength of their security systems.

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

The data security safeguards used by NAMIC member companies, which pre-date the GLBA and were developed on a voluntary basis, are consistent with the GLBA security standards prescribed to date. Those member companies that have affiliates in the banking and securities areas are familiar with the federal GLBA security guidelines, but for the insurance industry generally, the key source of guidance currently is the model security regulation recently adopted by the National Association of Insurance Commissioners ("NAIC"). The NAIC's model security regulation is patterned after the New York information security regulation (the only state GLBA security regulation currently in force), which in turn is modeled after the federal insurance information interagency guidelines. We anticipate that the NAIC model will become a regulation model for action by the various states over the coming months.

c. ***Do existing statutory and regulatory requirements protect information adequately?***

We believe the security standards set forth both in the federal interagency guidelines and the NAIC model are reasonable standards for securing the confidentiality of customer information. There are certain distinctions between the federal guidelines and the NAIC model with respect to company board responsibility, but both sets of standards share the key elements of a comprehensive customer information security program.

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

We believe it is premature to consider new statutory or regulatory security standards at this time. Both the federal GLBA guidelines and the NAIC information security model regulation are quite new. Financial institutions need time to review the consistency of their existing security systems with the new standards and then to implement any additional necessary security systems and test those new systems. Until this process is complete, we believe a moratorium on additional federal or state regulation is in the best interests of both consumers and regulated companies. Such a moratorium will permit the industry to coordinate with and appropriately adapt to other ongoing information security activities by various financial trade associations and the business community at large. In general, financial institutions need an opportunity to adapt to new technological advances becoming available to improve the physical, electronic and organizational safeguards for their customers' personal information.

Our concern about new statutory or regulatory privacy requirements is heightened by the requirements set out in the USA PATRIOT Act. This new law, unforeseen at the time that the GLBA was enacted, requires each insurer to develop anti-money laundering programs. The implications of the USA PATRIOT Act for information security systems remain unclear: while the statute provides an exception for data protection for GLBA compliance purposes, we are deeply concerned about balancing the privacy interests of our policyholders while complying with the USA PATRIOT Act. This is already a delicate task; new laws or regulations will only serve to further complicate our efforts. It is our belief that there should be a moratorium on any new data security rules for at least one year so that insurers and other financial institutions may have an opportunity to achieve a reasonable balance between GLBA and USA PATRIOT Act requirements.

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?***

We believe the potential risks to customer privacy from information sharing among financial institution affiliates are minimal. Sharing of customer information among affiliated companies is actually not significantly different from sharing the information within a single company itself. In general, many NAMIC member

companies that have affiliates use a single system for maintaining information gathered by all affiliated companies. The security safeguards in place ensure customer privacy because the shared systems have uniform physical, electronic and organizational safeguards.

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

We certainly recognize that there can be privacy risks associated with the sharing by a financial institution of customer information with nonaffiliated third parties. At the same time, it is clear that, for administrative and other functional reasons, customer information needs to be shared with such third parties. We believe the GLBA strikes the right balance in permitting sharing for these key purposes (as set forth in GLBA section 502(e)) while very strictly proscribing sharing for other purposes. Given the GLBA rules, we think financial institution customers face little risk to their privacy from the permissible sharing of the data they provide to their financial institutions. We note in particular that the GLBA permits a financial institution to share customer information with a nonaffiliated third party for service support or marketing purposes only if the institution, by contract, obligates the third party to maintain the confidentiality of the information and limits further disclosure of the information by the third party to only those disclosures that would be lawful if made directly by the financial institution (GLBA section 502(b)(2) & (c)).

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

We do not believe that, in general, a customer faces any greater risk to privacy when a financial institution shares customer information obtained from an affiliate than when the institution shares information obtained from a non-affiliated third party. We note, however, that in the rapidly decreasing number of cases of companies that maintain manual as opposed to automated information systems, transcription of or recording of information among affiliates could be inaccurate or incomplete. This is a similar risk in a nonelectronic or nonautomated exchange of information with a nonaffiliated third party.

4. The potential benefits for financial institutions and affiliates of such sharing of information.

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

The benefits to our member companies of sharing customer information with affiliates relate directly to the primary purpose of financial modernization under the GLBA: to permit the integration of financial services – insurance, banking and securities – so that financial institutions may serve consumers through a central point of contact. For many of our member companies, this benefit is realized in large part through the ability to cross-market appropriate products and services of their affiliates to existing customers.

In serving customers for their multiple financial services needs, sharing customer information among affiliated companies significantly reduces cost and improves accuracy in underwriting risks, handling claims and addressing customer concerns. Such information sharing is a critical element in identifying customer needs and thereby expanding consumer benefits from dealing with an integrated financial services organization.

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

Our member companies could not continue to function in the business of insurance without sharing customer information with nonaffiliated third parties. This is because, as noted, our companies daily rely on nonaffiliated third parties for assistance in the claim adjustment process, rating analyses, and the detection of fraud. Our response above to question 1(e) describes the importance and benefits of such data exchanges.

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

Our response above to question 1(d) describes the benefits to our member companies from the receipt of information shared with them by affiliated financial institutions.

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

The benefits to our member companies of sharing information obtained from their affiliates are not substantively different from the benefits of sharing information otherwise obtained. The original source of the customer information is not, at least for our member companies, a key determinant of the value of sharing the information with nonaffiliated third parties.

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

We believe that new and additional limitations on sharing of customer information with affiliates and nonaffiliated third parties would have significant adverse effects on our member companies and their affiliates, and accordingly, on NAMIC company policyholders. In our view, the regulations under Title V of the GLBA, as well as other state law privacy restrictions currently in place, provide a meaningful framework for protecting the privacy of insurance customers. We believe this existing regulatory framework appropriately balances the privacy protections of customers with the economic, convenience and other consumer benefits in an information-centered business environment. If our member companies were further restricted in sharing customer information with their affiliates, they could not effectively address customer demands and expectations with respect to efficiency, coordination, and integrated response systems. If insurers were further restricted in sharing customer information with nonaffiliated third parties, the business of insurance itself could be jeopardized, since, as discussed above, such third parties play critical roles in the insurance process, including (but not limited to) assisting in rating, claims settlement, data processing and fraud detection. In short, additional limitations on information sharing could unnecessarily deprive our member companies' customers of the very benefits – including both economic and convenience benefits – that the GLBA was designed to afford.

5. The potential benefits for sharing of information.

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

As noted above, financial institution customers expect the enterprise they deal with to know them and to assist them accordingly in addressing their individual needs. This is particularly true of insurance applicants and policyholders. Our members

companies tell us that their customers regard their insurance companies as a single entity, even though they may be organized as various subsidiaries under a holding company. Customers do not want to complete multiple applications, or to be underwritten without regard to current experience and transaction history with an organization as a whole. Rather, they expect application and billing information to be considered in their day-to-day dealings with an insurer on a total customer response basis.

Our member companies' customers benefit not only from the convenience that an integrated information system affords, but also from the significant cost-savings associated with such a system. With an integrated information system, an affiliated insurance company group can develop an appropriate, total insurance plan of protection for each individual customer, offering discounts related to multiple coverages and the experience of the individual with the entire affiliated enterprise.

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

Our member companies' customers benefit from the sharing of their information with nonaffiliated third parties every time a claim is presented and a loss is resolved more quickly because an auto repair shop or claim adjustment firm has access to customer information. Absent such sharing, insurance policyholders might ultimately bear the burden of resolving insurance claims on their own. Plainly, this is not what policyholders expect or need.

Our member companies' customers also benefit from sharing of their information with nonaffiliated third parties for the other fundamental insurance-related services described in our response above to question 1(e), including determinations of appropriate insurance rates and information processing. Without the assistance of nonaffiliated third parties working with customer data, our member companies, like other insurers, could not make these fundamental determinations for underwriting, rating and numerous administrative purposes.

In addition, as emphasized above, our member companies' customers also benefit significantly from the sharing of customer data with both affiliated and nonaffiliated third parties to detect and investigate fraud. It is important also to note the benefits of such sharing to help prevent identity theft. This benefit is of growing importance in light of the increased incidence and serious consequences of identity theft. The ability of financial institutions to help combat identity theft depends very substantially on their

access to and sharing of identification information with nonaffiliated third parties, since this enables them to avoid duplication in data dissemination and data inaccuracies (*e.g.*, with respect to customer addresses) that may inadvertently facilitate identity theft.

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

Customers benefit in the same ways when a financial institution shares with nonaffiliated third parties either (1) information that was obtained from one or more affiliates or (2) information otherwise obtained.

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

At least in the insurance context, we perceive no viable alternative for achieving the benefits that customers receive as a result of our member companies' sharing of customer information with both affiliates and nonaffiliated third parties. Simply put, such sharing is essential to allow our member companies to carry out the service and contractual promises they have made to their customers. As discussed further below, we do not believe there is any reason why customer interests in privacy cannot be satisfied while still permitting customers to benefit from affiliate and nonaffiliated party information sharing, particularly in light of the limitations and safeguards imposed under the GLBA and state law.

6. The adequacy of existing law 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?***

We believe existing privacy laws, including but not limited to the GLBA privacy regulations and the FCRA, do adequately protect the privacy of a customer's information. Indeed, as stated above, we believe that the FCRA opt-out provisions with respect to sharing of "consumer report" information among affiliates are more stringent than necessary to protect insurance customers. Given the breadth of the definition of "consumer report," the FCRA opt-out provisions impose notice burdens on insurers with respect to affiliates' sharing of such basic information as age, which is obviously an

important underwriting factor in some circumstances and which we believe customers expect our member companies to share with their affiliates for valid underwriting purposes.

In any event, we certainly do not believe there is any way in which existing privacy laws are *underprotective* of financial institution customers. Both the GLBA and the FCRA afford customers the right to prohibit financial institutions from sharing their personal information, and the complementary application of (1) the GLBA to sharing with nonaffiliated third parties and (2) the FCRA to sharing with affiliates makes the opt-out right comprehensive and meaningful in reality.

b. ***What about new laws?***

As indicated above, we do not perceive any benefit to customers that would be gained from new laws restricting information sharing by financial institutions, at least not at this time. The GLBA is still a relatively new statute and, particularly in the insurance context, where the state insurance regulators are still in the process of implementing the GLBA privacy requirements, it would be premature to move ahead now with any additional legal restrictions on financial institutions' information sharing. The GLBA and the FCRA are comprehensive complements with respect to customer privacy, and we believe they should be allowed to prove their adequacy through at least a five-year period without interference from any additional law. For this reason, we are particularly concerned about state legislation or regulation that goes beyond the GLBA and/or FCRA in the privacy area. We note, however, that we strongly support new legislation to extend the preemptive effect of the FCRA opt-out provisions and other FCRA provisions for which preemption of state law is due to expire as of January 1, 2004.

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

a. ***Have financial institution privacy notices been adequate in light of existing requirements?***

Our member companies have received few if any complaints or inquires about the privacy notice and policy statements provided to their customers. We note, however, that a task force of the NAIC is currently developing a model privacy notice designed to provide better guidance and be more "consumer friendly" and understandable than notices that track precisely the federal GLBA privacy regulations. Representatives of our member companies serve as part of the industry advisory group to the NAIC task force.

b. ***What about new laws?***

We do not believe new laws that would impose strict uniform mandates for the detailed form and language of privacy notices would be helpful or beneficial. Flexibility in both the method of delivery and the form of privacy notices is important because of the varied needs and structures of different financial institutions and their customers. A uniform "one-size-fits-all" methodology should be discouraged. We would urge that, as the federal regulators review this issue, they consider the functional state regulation to which our member companies are subject.

8. The feasibility of different approaches, including opt-out and opt-in, to permit customers 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 before sharing information with affiliates? With nonaffiliated third parties?***

A prior consent model is not a practicable mechanism with respect to financial institutions' information sharing with either affiliates or nonaffiliates. A requirement to obtain prior customer consent for information sharing with either affiliates or nonaffiliated third parties, while technically feasible, would result in significant limitations on the ability of financial institutions to serve their customers in a timely and effective manner. For insurers, the inevitable result would be increased costs, translated ultimately into increased premiums. This would run directly counter to the intended purpose of the GLBA: to facilitate more efficient and effective financial services for consumers through a more integrated financial services industry.

b. ***What about an opt in?***

We strongly oppose an opt-in model for information sharing with either affiliates or nonaffiliated third parties. The mechanisms for administering and processing insurance transactions are so varied and so dependent today upon sharing customer data with third parties that an opt-in would be highly unreasonable. Experience in other relevant contexts has shown that many if not most consumers will fail to exercise their right to opt-in to benefits simply due to passivity with respect to the steps required to opt-in. In the insurance context, an opt-in system would therefore effectively derail customer service. Claims would not be readily adjusted, data processing systems would need to be retooled at billions of dollars of cost, and Sally or John could not receive the claim draft

or repair on his or her car or home promptly. We believe an opt-in requirement would be a significant mistake for the financial industry generally and the insurance industry in particular.

* * *

We appreciate the opportunity to comment on the issues being addressed in the GLBA information sharing study. If you have any questions regarding our comments, please contact me by phone at (202) 942-5065, by fax at (202) 942-5999, or by e-mail to perkina@aporter.com.

Sincerely,

Nancy L. Perkins