21

Metropolitan Life Insurance Company
One Madison Avenue, New York, NY 10010-3690
212 578-2211

MetLife®

Ira Friedman
Senior Vice-President, Chief Privacy Officer and Special Counsel
Tel 212-578-3381 Fax 212-251-1668

April 22, 2002

Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, N.W.
Washington, D.C. 20552

Attn: Ms. Sandra Evans
Regulations and Legislation Division

Dear Ms. Evans:

Metropolitan Life Insurance Company (MetLife) is pleased to submit these comments, on behalf of itself and its affiliates, on the issues which the Treasury Department ("Treasury") raised in the Notice and request for comments dated February 4, 2002 in connection with Treasury's study of information-sharing practices among financial institutions and their affiliates, as required by Title V of the Gramm-Leach-Bliley Act of 1999 ("GLBA").

MetLife and its affiliated companies in the MetLife, Inc. group are a leading provider of insurance and financial products and services to a broad spectrum of individual and institutional customers. MetLife, with $282.4 billion of assets under management as of December 31, 2001, provides individual insurance and investment products to approximately 10 million households in the U.S. MetLife is also the largest provider of group life insurance to corporations and other institutions in the U.S., and we provide pension and retirement savings plans to that market as well.

General Comment

When we speak to our employees at MetLife about protecting customer information, we start with a Privacy Golden Rule: We should treat our customers the way we ourselves want to be treated as customers. True, customer information must be protected because the law requires it. But at MetLife, it is even more important to protect customer information because our business principles require it. And we think that all responsible financial institutions are driven by the same business imperative. Improperly disclose customer information, and you risk losing customer trust. Lose customer trust, and you can lose business. It's that simple.

So, at MetLife, we support the principles underlying Title V of the GLBA. In fact, we have taken steps that neither the GLBA nor any other law require. Mindful of public

concern about information disclosure to nonaffiliated third parties, MetLife has chosen to limit the disclosure of customer information to such parties to the situations where the GLBA permits disclosures without going to the customer first. In effect, we have "opted out" on behalf of our customers with respect to the sharing of information for those purposes for which the GLBA requires that customers be given the choice to opt out. Other financial institutions have done the same.

In addition, we understand that a customer's health information is particularly sensitive. So, we have stated as a matter of policy that we will not disclose customer health information, even among affiliates, for marketing purposes unless the customer consents.

We believe that Congress struck the right balance in the GLBA (and other privacy laws) between the need to protect customer information and the need to allow companies to share that information for a range of legitimate purposes. Where disclosures are made, they help the financial institution better meet the needs of its customers and the needs of public health and safety.

We do not believe that further restrictions on information sharing among the affiliates of financial institutions are warranted or wise. As we explain in our specific responses below, customers and other consumers stand to benefit from the ability of affiliated financial institutions to share information about them. Conversely, customers and other consumers stand not only to lose those benefits, but actually to experience higher expense-driven costs, if tighter restrictions are imposed.

We believe it was unfortunate that the GLBA left the gates open for states to compete with each other to outdo the GLBA in consumer protection. The result may well be significant additional compliance expense without any real demonstration that there are any additional "protections" or that they are meeting a true need. And state-to-state variations in privacy notices are likely to lead to even greater confusion among consumers about the way in which any privacy concerns they may have are being addressed.

Specific Responses

Our specific responses are set forth in the following pages. In accordance with the instructions in Treasury's request for comments, each of MetLife's responses to the questions raised by Treasury is identified with the number and letter to which the response relates. For convenience and clarity, Treasury's questions are restated in bold type with our response below.

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

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

Like many of the country's largest life insurance companies, MetLife and its affiliates are all either financial institutions or companies whose operations are closely related to, if not incidental to, the financial services business.

MetLife and its affiliates share information with each other for one or more of the following purposes:

- To enable the MetLife affiliates to service and help administer each other's business under inter-affiliate administrative arrangements and to verify customer information.

- To allow the MetLife, Inc. group of affiliated companies to offer their customers the benefit of one-stop shopping for a wide range of financial products and services, mainly insurance, mutual fund and banking services.

- In the case of property and casualty insurance, it is common practice to engage in the auto insurance business through an affiliated group of companies, each of which insures comparably rated risks – preferred, standard and nonstandard. The application may be submitted to any of several affiliated companies to determine which one will offer to issue the insurance policy. This helps assure that the risk is properly underwritten and priced. (It also helps assure the company's customers that they will not have to pay higher premiums in order to subsidize higher risk customers.)

Typically, the information shared would include basic information about the customer – name, address, age, and other contact information – and may include social security numbers or other identification numbers, as well as financial and rating information obtained in the course of processing applications and other transactions with the customer and verifying information about the customer.

MetLife and its affiliates have adopted a corporate policy that prohibits the disclosure of customer health information among affiliates for marketing purposes unless the customer consents.

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

Title V of the GLBA recognizes that there are many appropriate circumstances under which life insurance companies may share customer information with nonaffiliated entities. For example, life insurance companies may engage the services of nonaffiliated third parties to assist them in processing customer applications, claims and other customer transactions. Or companies may outsource

entire functions like underwriting and claims administration, where it can be shown that such functions can be performed at least as well, but less expensively, by outside firms. In order to be able to service the life insurance company, the third party must typically have access to relevant customer information.

It would be a rare life insurance company that does not use nonaffiliated third parties to verify information provided by customers and others. Among other benefits to customers, these information disclosures help prevent identify theft because they enable the company to confirm that individuals asking for customer information have correctly identified themselves.

Also, in the ordinary course of their business, life insurance companies typically spread their risks through reinsurance purchased from nonaffiliated third parties, and customer information may have to be provided to the reinsurance companies so that they can assess their risk and audit reported losses.

It should be noted that MetLife and some of its affiliates engage in businesses that are subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). As such, MetLife and its affected affiliates will have to assure that the administrative, technical and physical safeguards that are in place with respect to "personal health information" meet the requirements of HIPAA. MetLife and its affected affiliates will also be required to enter into HIPAA-compliant "business associate" contracts with affiliates and nonaffiliated third parties that service or help administer their HIPAA-regulated businesses.

Like all other companies, MetLife must from time to time provide customer information in response to lawsuits or regulatory examinations. Moreover, customer information must be disclosed from time to time to governmental and non-governmental third parties for reasons of public health and safety. For example, several states have laws requiring the disclosure of communicable disease cases to a state agency, and various states require the disclosure of positive HIV results to a physician. Similarly, disclosures of customer information may have to be made under such laws as the Provide Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (PATRIOT Act).

At the same time, mindful of public concern about information disclosure to nonaffiliated third parties, MetLife has chosen to limit the disclosure of customer information to such parties to the situations described above (except for joint marketing agreements as permitted by the GLBA). In effect, we have "opted out" on behalf of our customers with respect to the sharing of information for purposes for which the GLBA requires that customers be given the choice to opt out.

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.

MetLife and other life insurance companies commonly use nonaffiliates, and in many cases affiliates, to service and help administer their business. Essentially the same disclosures are made for such purposes, regardless of whether the other party is an affiliate or a nonaffiliate.

Also, MetLife and various other financial institutions have decided, as a matter of policy, not to share customer information with nonaffiliated parties to help those parties market their products and services, unless the customer consents.

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

At MetLife, customer information may be shared with affiliates in order to enable them to service and help administer each other's business and to verify customer information. Information sharing among affiliates also makes convenient one-stop shopping possible, usually through a single insurance agent who is familiar with all the customer's needs as they change over time. And in the auto insurance business, it is common practice to submit the consumer's application to any of several affiliated companies to determine which one will offer to issue the insurance policy at a premium rate that is appropriate, given the risk insured; this helps assure that the risk is properly underwritten and priced and that customers with better driving records are not paying higher premiums in order to subsidize losses on policies issued to higher risk drivers.

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

Customer information may be shared with unaffiliated third parties that help service our products, to verify information and prevent identify theft and other types of fraud, to share risks with reinsurance companies, and for other purposes required or permitted by law.

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

MetLife and its affiliates have adopted a corporate policy that prohibits the disclosure of customer health information among affiliates for marketing purposes unless the customer consents.

MetLife (and other financial institutions) have chosen to limit the disclosure of customer information to nonaffiliated third parties to the situations where the GLBA authorizes disclosures without providing an "opt out" choice.

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

Federal and state telemarketing laws prohibit companies from making telemarketing calls to individuals who have requested that their telephone numbers be placed on a company or state "do not call" list. As a practical matter, this may limit the inter-affiliate sharing for marketing purposes of information about those customers who have placed themselves on such a list.

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?

We believe that the GLBA gives us the flexibility to share information as warranted, and we have no comment on this question.

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

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

As noted above, the GLBA requires financial institutions to protect the security and confidentiality of a customer's "non-public personal information." The GLBA also directs those governmental agencies that regulate financial institutions to establish standards for administrative, technical and physical safeguards in order to:

(1) ensure the security and confidentiality of customer records and information containing nonpublic personal information;

(2) protect against any anticipated threats or hazards to the security or integrity of such records and information; and

(3) protect against unauthorized access to or use of such records which could result in substantial harm or inconvenience to any customer.

MetLife has long-standing policies, standards and practices to help assure information security. Like many other companies, we recognized long before the GLBA was enacted that our computer systems, applications and data bases could be vulnerable to a variety of threats, particularly as invasive technology became more sophisticated and available. We take reasonable steps to assure that our policies and standards in this regard remain up-to-date. An internal committee with representation from technology, law, human resources and other interested departments helps oversee our technology security policies, standards and practices.

We also communicate regularly to our employees concerning company standards that relate to confidentiality. For example, we periodically remind our employees (and others who may have access to our computer systems, applications and data bases) that customer information and other information owned by the company, or communicated to it with an expectation of confidentiality, must be used appropriately and must be kept confidential. In addition, we require third parties to whom confidential information is communicated in the course of business dealings to safeguard that information from unauthorized disclosure.

MetLife is also protecting the security of information on paper or maintained in other media. In fact, we are preparing to publish a comprehensive information security guide for managers and our general employee population that will pull together and enhance our current policies.

The following is a description of some of the safeguards MetLife currently has in place with respect to information security in general:

- A written policy, reinforced by training programs, instructing all employees to treat non-public personal information as confidential and subjecting employees to disciplinary action if they fail to do so.

- A requirement that terminated employees return all company records (including records on computers for employee use).

- Publication of policies on MetLife 's intranet website, making them readily available to all employees.

- Protection of electronic records through the use of multiple computer software products that employ such security features as passwords, user identification numbers, and personal identification numbers to guard against unauthorized access.

The following are examples of safeguards that MetLife currently maintains in order to protect against anticipated threats or hazards to the security and integrity of such records and information.

- Limiting building access to employees with appropriate identification and to authorized visitors.

- Internal systems containing electronic "secure" firewalls, surveillance software and other security measures designed to prevent unauthorized access to electronic records.

- Electronic points of entry, as well as databases, servers, e-mail and workstations protected by virus detection/removal software.

In addition, MetLife's internal auditors conduct periodic audits aimed at testing the systems controls in order to help assure compliance with these policies and standards, identify and assess risk and develop controls to mitigate risk.

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

The GLBA does not detail the lengths to which financial institutions must go in order to put in place administrative, technical and physical safeguards. It is clear from the implementing regulations that federal and state authorities are promulgating that the safeguards must be sufficient, based on an assessment of risks. Many financial institutions build redundant protection and take other measures that go beyond the minimum needed to comply with the GLBA. We do so, not because the law requires it, but because we are very focused on assuring customer satisfaction and on the need to protect customer information as a business imperative.

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

We believe that the GLBA strikes an appropriate balance between the need to protect customer information and the need to allow companies to share that information for a range of legitimate purposes. Where disclosures are made, they help the financial institution better meet the needs of its customers, serve the needs of public health and safety or enable financial institutions to comply with the law.

Regulation in this area works best when it prescribes broad standards and leaves it to the regulated companies to decide how best to meet those standards. Life

insurance companies, in particular, are generally subject to regulatory examination to determine whether those standards are met. This approach is appropriate.

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

Given the requirements of the GLBA, HIPAA and the numerous other Federal and state laws that address privacy, no new or revised protections are needed.

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?

If a financial institution is complying with the GLBA and all other applicable laws, customers do not face any meaningful risk when the financial institution shares the customer's information with an affiliate.

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

Whatever the potential privacy risks may be when a financial institution shares the customer's information with a nonaffiliated third party, we believe that the GLBA "opt out" requirement is appropriate and sufficient to protect customers from them.

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

We do not understand the significance from a privacy risk perspective of the information passing from one affiliate to another affiliate and then to a nonaffiliated third party. At MetLife, and at the other financial institutions we know about, the Chief Privacy Officer oversees the implementation of and compliance with privacy policy throughout the entire affiliated group of companies. The risk dynamics do not change simply because one affiliate has disclosed customer information to another affiliate which, in turn, discloses the information to a nonaffiliate. Essentially the same protective privacy policies apply throughout.

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

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

Life insurance companies can serve the customer's existing and potential needs more efficiently and cost-effectively by sharing customer information. For example, many life insurance companies have found that it is more efficient and cost-effective to establish a common back office that processes applications, transactions and claims for customers. The savings generated by these efficiencies enable the life insurance company to pass on a portion of those savings to its customers.

In addition, expanding product relationships with existing customers has become an essential business model for many financial institutions throughout the country. This strategy enables the financial institution to generate additional business from its own customers as well as those of its affiliates.

We have found that our customers value a relationship with a single account executive who will get to know their needs, call their attention to other products and services offered by MetLife and its affiliates, and become their trusted advisor as their financial needs change over time.

In the case of property and casualty companies, it is common practice to engage in the auto insurance business through an affiliated group of companies, each of which insures comparably rated risks – preferred, standard and nonstandard. The application may be submitted to any of several affiliated companies to determine which one will offer to issue the insurance policy. This helps assure that the risk is properly underwritten and priced. (It also helps assure the insurance buyer that she will not have to pay higher premiums in order to subsidize higher risk customers.)

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

It is increasingly common and beneficial for financial institutions to outsource certain customer services to nonaffiliated parties; such outsourcing may entail the sharing of customer information with such parties. For example, nonaffiliates may be engaged by life insurance companies to act as third-party administrators of particular segments of business because they have more expertise and/or scale to perform the function more efficiently and cost-effectively.

In addition, as the GLBA appropriately recognizes, financial institutions may engage in joint marketing with nonaffiliated companies.

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

Affiliates generally benefit in the same fashion as the financial institution.

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

Affiliates generally benefit in the same fashion as the financial institution. We see no reason to distinguish between the ability of a financial institution to share customer information with its affiliates and the ability of one affiliate to share such information received from the financial institution with another affiliate.

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

Further limitations on the sharing of information among affiliates could seriously undermine the ability of companies to broaden their relationship with customers by offering multi-product, one-stop shopping across affiliates. Moreover, further restrictions could get in the way of outsourcing services, consolidating back offices and giving the customers the personal attention and care they get when all their financial needs are being serviced by a single trusted advisor.

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

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

Customers benefit in quite a few ways from the sharing of customer information among the insurance company's affiliates:

1) Quicker, more efficient service when back office operations of various affiliates are consolidated and can take advantage of scale.

2) Consolidated back offices cut expenses, a savings that can be shared with customers in the form of lower prices.

3) One-stop shopping, whereby an affiliated group of companies can efficiently offer the customer a range of products and services that will meet all of the customer's financial needs.

4) A single account executive who knows the customer's needs, particularly as they change over time, and serves as a trusted advisor who helps the customer plan for the future.

5) In the case of car insurance, the proper underwriting and pricing of the risk, and its assignment to the affiliate that insures risks within a comparable range, means that customers who are better risks are not subsidizing higher risk customers.

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

Customers benefit in various ways from the sharing of customer information with nonaffiliated third parties:

1) The ability to outsource services enables financial institutions to provide quicker, more efficient service to the customer, and to share with the customer the savings that result from the outsourcing.

2) Companies that provide these services are often more familiar with best practices in their areas of expertise, and they employ those best practices to the benefit of the customers they service.

3) Prevention of fraud, and the ability to make disclosures that are reasonably necessary to protect the public health and safety, have never been more important than they are today. It would, for example, be ironic if laws passed to protect customers against identity theft had the effect of making it easier for others to steal identities and fraudulently obtain goods and services.

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

We do not see any meaningful distinction to be made based on whether the original source of the information was another affiliate or a nonaffiliated third party.

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

The case for further restrictions on the disclosure of customer information simply has not been made. To the contrary, restrictions that go beyond what current law provides may have a "chilling effect" on business, interfering with the ability to service customers and imposing limitations that do not really benefit the consumer.

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

Further limitations will interfere with the ability of business to provide customers with the benefits outlined in response to Question 5.

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

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

With the passage of the GLBA, HIPAA, FCRA and various other federal and state privacy laws, consumers have far greater protection of their privacy when they deal with financial institutions than they have in dealings with any other type of business.

Turning to the laws in their own right, existing privacy laws adequately protect the privacy of customer information. The GLBA, FCRA and various state laws provide four key privacy protections to customers. These are:

1) Notice – Financial institutions have an obligation to provide customers with a notice of the institution's information practices.

2) Choice – Since customers are made aware of a financial institution's information practices, each customer has a very powerful choice – whether, in light of those practices, he or she wishes to do business with that financial institution. If a customer decides to do business with MetLife, we believe that the customer must have concluded that MetLife is making reasonable uses and disclosures of customer information, and that such disclosures are needed in order to provide efficient and accurate service to the customer and to protect the interests of the company and its customers generally. The privacy laws recognize this by permitting information to be disclosed for legitimate business purposes, such as to a third party who provides administrative services for a life insurance company.

We do not believe that a customer would reasonably anticipate that a life insurance company would disclose the customer's information to a nonaffiliated third party to enable the third party to market products and services to the customer. That is precisely why a customer should have the right to tell a life insurance company not to share information in this way. At

MetLife, we took the additional step of opting out for our customers by deciding as a policy matter not to share customer information with nonaffiliates to help them market their products and services.

3) Safeguarding Customer Information - The regulations promulgated pursuant to §501 of the GLBA require financial institutions to put administrative, technical and physical safeguards in place to adequately protect customer information. This affirmative responsibility to safeguard customer information was an important addition to customer privacy protection since this is one area that had not been adequately addressed by previous customer privacy laws.

4) Access and Correction – Both FCRA and, in the case of insurers, state law, provide a customer with a right of access to certain information maintained about her and the opportunity to dispute the accuracy of information and to correct inaccurate information.

We believe that taken together, these four privacy protections adequately protect the privacy of customers because they establish a fair information relationship between the customer and the financial institution and provide a reasonable degree of confidentiality with respect to the information collected. They also recognize the interests of all customers in information practices that: (i) allow financial institutions to provide services accurately and efficiently; and (ii) do not unduly restrict the sharing of information necessary to, for example, prevent and detect unlawful activities such as insurance fraud, or enhance domestic security against terrorism as permitted under the Patriot Act.

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

The GLBA should be amended to prevent states from passing more restrictive privacy laws than GLBA and HIPAA. Ironically, there are already signs that opening the gates to more restrictive state laws will lead to a multitude of confusing requirements. In the end, it is not at all clear that those laws (for example, in California and New Mexico) will increase privacy protection. What is clear is that they will significantly increase the cost of compliance, both to the companies and to their customers, and that those additional requirements are likely to result in notices that confuse, not clarify, what the privacy protections are.

Today, financial services is almost entirely interstate commerce. Companies facing a multitude of inconsistent state laws have to spend the time and money to track those laws, make technology and process modifications to accommodate their requirements, and translate a hodgepodge of requirements into one or more notices that make sense of it all for consumers. If that isn't enough to raise the cost of

doing business, companies will also have to worry about the legal risk of not fully complying with each of the state's laws. (Already, companies are greatly confused by different state health information laws and the need to determine which laws exceed the requirements of HIPAA and require special attention.) The result will be more expenses to pass on to consumers, thus costing consumers, not benefiting them.

State-by-state variations in privacy requirements will inevitably lead to multiple, confusing privacy notices. Consumers already complain that the notices they receive are complex and incomprehensible, and they may well be right about that. However, ironically, inconsistent state laws will aggravate this problem.

The GLBA privacy notices that were first sent to consumers in 2001 may have been too complex and not as easy to understand as they might have been. That is because the GLBA, and HIPAA, require that the notices fully inform consumers of what the laws say and what all of their rights are. As a result, companies felt they had to make sure they covered all the points in the law, which made for somewhat long and detailed notices.

It appears now that policymakers are beginning to acknowledge that simpler notices, giving consumers just the information that is most important to them, will in the end be more meaningful than notices that read like the laws and regulations themselves. And financial institutions do want to tell their customers how the company is protecting their information and do want to communicate in a meaningful, understandable way.

Unfortunately, it appears that the states have already begun to compete to see which state can impose the greatest number of limitations on companies, the most rights for consumers, and the most sophisticated form of notice. This is not good news for consumers. The result will be even more complex notices, and a multitude of different notices from companies based in different states and operating on a multi-state scale.

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

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

b. What, if any, new or revised requirements would improve how financial institutions describe their privacy policies and practices and inform customers about their privacy rights? Please explain how any of these

new or revised requirements would improve financial institutions' notices.

This is in response to both parts of this Question 7. As a general matter, we believe that the notices utilized by insurance companies have been adequate in light of existing requirements. As a result of state laws, many insurance companies have been providing privacy notices to customers for over twenty years. Accordingly, many insurers have experience in complying with privacy notice requirements. We would also point out that to comply with the GLBA's requirement to send all existing customers a privacy notice, financial institutions mailed *hundreds of millions* of notices. For many companies, the number of customer inquiries related to the notice was minimal. While some commentators claim that the this feedback rate was low because the notices were overly complex or simply not readable, we believe that the average consumer simply does not feel at risk because financial institutions share information with affiliates and nonaffiliates. Consumers trust their banks, insurance companies and securities firms to handle their information with care, and with rare exception that trust is justified.

We do strongly suggest is that consideration be given to eliminating the annual notice requirement of the GLBA. Financial institutions want to tell their customers how the company is protecting their information, and they want to communicate to their customers in a meaningful, understandable way. And we believe it is very important to inform a customer of a financial institution's information practices at the start of the customer relationship. However, absent a change in an institution's practices, merely repeating the same information on yearly basis does not appear to serve a useful purpose. Worse, we believe that receiving a yearly notice from numerous financial institutions with which the customer does business may just annoy the customer. In particular, life insurance customers whose policies have been in effect for many years may get unnecessarily concerned that these mailings mean that something is happening to their insurance coverage. We believe that eliminating the annual notice requirement (thus cutting down on the number of notices that a customer receives) may increase the amount of customer attention to each institution's notice and may thereby increase customer understanding of privacy rights.

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 (opt in) before sharing information with affiliates in some or all circumstances? With nonaffiliated third parties? Please explain what effects, both positive and negative, such a requirement would have on financial

institutions and on consumers.

An opt-in process may be feasible, but it will unduly disrupt the way many financial institutions do business. All the information we have indicates that the vast majority of customers will fail to respond simply because they tend not to pay attention to such matters. And, by inaction, they will be deprived of the benefits we have described in response to Question 5. It will be expensive to administer, meaning a higher cost that will be passed on to the consumer.

We see no reason to distinguish between affiliates and nonaffiliates in this regard. An "opt-in" regime is simply too restrictive and can have a "chilling effect" on legitimate disclosures of information.

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

Financial institutions should be, and currently are, permitted to adopt policies that prohibit the sharing of information, with affiliates or with nonaffiliates. At least one leading life insurance company has adopted a policy that prohibits the sharing of health, both with affiliates and with nonaffiliates, for the purpose of marketing the other company's products, unless the customer consents.

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

While it may be feasible to impose this requirement, it would not be reasonable or appropriate to do so. Financial institutions will, of course, incur whatever expenses and other burdens are necessary to comply with any change in the law. However, as noted in response to previous questions, financial institutions are typically affiliated only with other financial institutions or companies whose businesses are closely related to, if not incidental to, financial services. This does not present a risk of abuse of any significance. Moreover, we have seen little, if any, evidence that more than a small minority of consumers are concerned about information sharing among affiliates of financial institutions.

We see no positive effect that would come from such a requirement. Quite to the contrary: it would be burdensome, and expensive for the companies, and few consumers would take advantage of it.

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

Some customers, albeit a small number, are already telling companies that they do not want their information shared with the company's affiliates. Our impression is that quite a few companies are taking reasonable steps to accommodate those requests, even though the law does not require them to do so. While these companies cannot fully comply with such "do not share" requests without making expensive systems modifications, they are doing the next best thing: putting the customer on their "do not call" lists. This will cut down significantly on the possibility that the customer's information will be shared for marketing purposes among affiliates, which is probably the main goal that the customer wanted to achieve.

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

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

Unfortunately, enabling the customer to restrict information sharing to certain purposes – for example, customers may be willing to hear from certain types of affiliates, or about certain types of products, but not others – would require extensive and expensive systems modifications. Also, many customers get confused when they have too many choices.

Some companies may choose to give their customers a variety of choices. However, the law should not mandate it.

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

We believe the preceding response answers this question as well.

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

We have no experience to report.

Again, thank you for this opportunity and for your kind attention to these comments.

Very truly yours

Ira Friedman
Senior Vice-President,
Chief Privacy Officer
and Special Counsel