32

THE FINANCIAL SERVICES ROUNDTABLE

May 1, 2002

Sheila C. Bair
Assistant Secretary of the Treasury
c/o Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, N.W.
Washington, D.C. 20552

ATTN: Study on GLBA Information Sharing

Re: Comments on the GLBA Information Sharing Study

Dear Assistant Secretary Bair:

The Financial Services Roundtable ("The Roundtablc") appreciates the opportunity to comment to the Treasury Department, the federal functional regulatory agencies, and the Federal Trade Commission, on the study on information sharing practices among financial institutions and their affiliates, as required by Title V of the Gramm-Leach-Bliley Act of 1999 ("GLB Act"). The Roundtable is a national association representing 100 of the largest integrated financial services firms providing banking, insurance, and investment products and services to American consumers.

The Roundtable submits the following three-part response to the Treasury Department. The first part is this letter, a brief, but comprehensive, executive summary of the key points that the Roundtable wishes to be considered. The second part is an addendum to this letter, which consists of our general comments and specific responses to the questions presented in the Treasury's request for comments. The third part is a Survey of our member companies conducted by Ernst & Young, *Customer Benefits from Current Information Sharing by Financial Services Companies*, which demonstrates and quantifies the real benefits to consumers of information sharing.

Consumers Benefit From Information Sharing

As the steam engine drove the Industrial Revolution, information technology is propelling the U.S. economy to new heights. Information technology, which is the use, management, and/or integration of customer information by business firms, has led to dramatically increased value for consumers, especially consumers of financial services. For instance, a recent study by Kitchenman in 1999 (Kitchenman, W. (1999) "US Credit Reporting: Perceived Benefits Outweigh Privacy Concerns," The Tower Group (January).), suggests that mortgage rates in the U.S. are, on average, two percentage points less costly than elsewhere. These startling savings must, in some significant measure, be due to the efficient management by lenders of enormous amounts of information about borrowers. Likewise, U.S. consumers, at almost all levels of the economic spectrum, have access to credit, often instantaneously, a phenomenon that does not exist in other developed countries and that is made possible by the integration of personal information.

The benefits to customers of information sharing by financial services firms are significant. As the Roundtable member Survey demonstrates, customers benefit from increased convenience, personalized service, and real savings of time and money. Consumers demand and benefit from conveniences such as internet banking, automatic teller machines, call centers and toll-free customer support services, relationship pricing and services, and consolidated monthly statements, all of which are the result of information sharing and its management. As noted below, consumers also benefit from information sharing through the prevention of fraud and identity theft.

The Roundtable's E&Y Survey demonstrates that information sharing results in the following benefits, for customers of Roundtable members, among others:

- $17 Billion in savings per year, and
- 320 million hours of time savings per year.

These numbers will be dramatically larger if all financial firms are included.

Our discussions with consumer groups about the results of our Survey indicate that the direct benefits of information sharing are not understood or appreciated by the public. As the benefits were explained to the consumers, they favored information sharing with the protections of the GLB Act and best industry practices.

A National Uniform Privacy Standard is Crucial

It is critically important to the economy, to consumers, and to the financial services industry that the U.S. have a national uniform privacy standard. The Roundtable member companies support a standard that is a balance between protecting customers'

expectations of financial privacy, on the one hand, and security and allowing companies to share information in order to provide consumers with lower cost products, convenience, and more comprehensive services, on the other hand. Anything less than a uniform national privacy standard jeopardizes the very real benefits that U.S. consumers, the economy, and the industry receive from information sharing.

As integrated financial services providers, Roundtable members are full-service financial services firms and have complex legal and operating structures. These complex structures are based, in part, on the requirements of the statutory framework under which they operate and, in part, on different methods for providing products and services to customers. Importantly, no two of these structures are necessarily alike.

Roundtable member firms serve consumers in many states. Therefore, differing state laws that limit or restrict the flow of information within a corporate family would, we believe, have damaging consequences. An integrated database that incorporates customer financial information across affiliates, business lines, and third-party service providers is an important instrument that better enables our members to detect and prevent fraud, to provide multiple and expected benefits to consumers, and to track efficiently and effectively the flow of criminal funds.

The most important tools that financial firms have available to fight fraud and assist governmental efforts to catch criminals are:

- a sophisticated and integrated database that incorporates customer information across all of a firm's retail businesses; and
- a vigilant customer service staff, especially the bank tellers and others, who are the front line of any firm's defense against fraud and identity theft.

These tools would be jeopardized by unwise restrictions that set different standards, require multiple or non-integrated databases, prohibit the use of common identifiers such as social security numbers, or restrict the basic sharing of information. A federal law should establish standards that are consistent throughout our nation.

Because the flow of information does not stop at state borders, even one state law that differs from existing federal standards sows confusion for consumers. In addition, conflicting state laws are impractical and diminish consumer benefits and protections.

Several precedents exist for a national uniform privacy standard, including:

- The laws providing federal charters for banks, thrifts, and credit unions.
- The preemption of state usury laws;
- The Fair Credit Reporting Act;
- The Truth-In-Lending Act; and

Addendum: General Comments and Responses to Questions

In its request for comment, the Treasury Department solicited responses to a series of specific questions and any other issues relevant to the study. The Roundtable sets forth below its general comments on these issues and its specific responses to the numbered questions, as presented in the Treasury's request for comment.

General Comments

Information Sharing Results in Real Consumer Benefits.

For many years, customers of financial services firms have provided information to their financial institution in order to obtain products or services with the expectation that the firm will use the information wisely and protect the confidentiality of that information. From every survey that we are aware of, customers generally continue to trust their financial firms. What customers may not expect or realize is that real, quantifiable benefits are the direct product of information sharing within a firm, including its affiliates, its third-party service providers, and its marketing partners. The Fair Credit Reporting Act ("FCRA") and the Gramm-Leach-Bliley Act ("GLB Act") currently permit the integration of customer information.

Consumers demand and expect:

- Low-cost credit availability;
- Convenience in the application process for credit, insurance, and other financial products;
- Personalized services;
- The option of one-stop service providers;
- Time savings and convenience;
- More product and service options;
- Protection from identity theft; and
- Protection from fraud.

The Roundtable commissioned a survey by Ernst & Young, *Customer Benefits from Current Information Sharing by Financial Services Companies*, dated December 20, 2000, which demonstrates and quantifies significant benefits to customers. These benefits include increased convenience, personalized service, and real savings of time and money. The Survey, the results of which are detailed in the "Specific Responses" section below, is attached. E&Y surveyed a sampling of Roundtable member companies because the companies know how much information is shared for different purposes, why

information is shared, and the benefits provided to consumers—all of which are virtually unknown by most consumers.

After the E&Y Survey, the Roundtable conducted informal consumer group discussions about the Survey and its results. We discovered that each of the above benefits is often invisible to consumers. These groups suggest that customers initially do not understand or appreciate how information sharing makes each of the above benefits possible. Nonetheless, these benefits are real and substantial.

A Uniform National Standard Promotes Benefits.

As noted above, real benefits result from the information sharing that is currently permitted, while existing confidentiality protections and security safeguards protect the privacy of customer information. These benefits are the direct product of the current uniform national standard for information usage as provided by the Fair Credit Reporting Act. In addition, the wide availability of financial products and services is a national resource that is also the product of information sharing.

Different and inconsistent laws passed by states and localities would reduce the benefits already available and may eliminate potential future benefits. Differing jurisdictional requirements would add unnecessary costs and confuse consumers. We fail to see how the added burden of different requirements would produce the benefits to consumers in obtaining the financial products and services they desire on a low cost and convenient basis or incrementally enhance privacy beyond the protections provided by the GLB Act and the Fair Credit Reporting Act.

With regard to the authority for states to impose requirements different from the standard set in the GLB Act, it is important to note the status of states in the opt-in/opt-out debate. In Vermont, due to regulatory requirements imposed by the Commissioner, who regulates insurance, banks, and securities firms, financial institutions may have to develop an opt-in mechanism (currently under challenge in State Court) if they intend to disclose nonpublic personal information to nonaffiliated third parties to allow marketing of that institution's financial products and services. Insurers (but not other financial institutions) will have to do the same in New Mexico, and interpretation of the Montana statute is still under discussion. For a number of years, Minnesota has prohibited sharing of personal information by insurers with affiliates for marketing of non-insurance products and with nonaffiliates for marketing any type of product. In California, the governor and legislative leadership all profess support for restrictions beyond those imposed by the GLB Act, including some form of opt-in for disclosure of certain information.

Why Financial Services Firms Offer Products Through Different Channels

The Roundtable's membership is very diverse, both in terms of its product and service offerings and the corporate structures under which its various members operate. Thus, it may be useful to describe the manner in which our members are organized and how they provide products and services to their customers. This explanation should be particularly useful in understanding what information is shared, and for what purposes, among the relevant entities. It should also be noted that the following discussion is equally applicable to financial service firms that are not Roundtable members.

In this regard, there are three types of relational entities that Roundtable members use to provide products and services to their customers: affiliates, which are wholly owned corporate entities; third-party service providers; and marketing partners.

<u>Affiliates</u>. First, the existing statutory framework dictates that full-service, integrated firms may offer banking, securities, and insurance products only through a group of affiliates under common ownership, but not within a single corporate entity. For public policy reasons, this country has not embraced a universal financial services model; rather we have maintained a separate affiliate approach. This was confirmed most recently with enactment of the GLB Act, which authorized for the first time the affiliation of full-service banks (including thrifts), securities firms, insurance companies, and investment companies under the umbrella of a financial services holding company.

An affiliate is a separately incorporated entity with all of the characteristics of a corporation and is wholly owned or controlled by its corporate parent. Each affiliated company within the same financial holding company remains regulated by its primary functional regulator. Many of our member companies have hundreds of affiliates, and many of those affiliates may interact with the same individual retail customers.

Second, the manner in which financial services firms operate varies tremendously; there is no typical model. As noted above, the GLB Act requires integrated financial services firms to conduct banking, securities, and insurance activities through separate affiliates. However, some firms may operate separate corporate entities, such as banks, mortgage companies, or insurance companies on a state-by-state basis. In addition, some products may be offered by a bank, a subsidiary of the bank, or an affiliate of the parent firm. For example, a firm may choose to offer mortgage products through a bank, through a subsidiary of another bank, and/or through an affiliated mortgage company.

There are numerous reasons why different firms choose to offer products through different entities. They include:

- Technical regulatory, including licensing, requirements;
- Taxation;
- Historical;
- Capital allocation methodologies;
- Compensation;
- Capitalizing on local name or brand recognition;
- Market segmentation; and
- Managerial.

Thus, a financial product may be offered through one type of entity in one organization, while the same product is offered through one or more different entities in another organization. For example, a bank holding company may offer all of its mortgage products directly through one of its bank subsidiaries, while another holding company may offer mortgage products only through one or more of its non-bank subsidiaries, such as a mortgage company or finance company. For efficiency, the underwriting of credit or insurance, or the billing, collection, and servicing of customer accounts may be provided by a single affiliate on behalf of several affiliated companies.

Financial services firms also vary greatly in how certain services are provided both internally, for themselves, and externally, for their customers. Services may be provided through one or more affiliates of the organization. (Financial firms also may provide services through a third-party provider, as discussed below.) For example, one firm may choose to provide internal services, such as check printing, loan servicing or collections, through one or more affiliates. Similarly, one firm may choose to specialize and provide all external customer services through one affiliate, while another firm may provide individual customer services through individual affiliates. Considerations such as cost, efficiency, and technical regulatory requirements, such as licensing laws, are among the reasons a company may choose different distribution channels for its products and services. For both types of services, firms are required to internally manage information consistent with the confidentiality obligations established by the GLB Act.

Third-Party Service Providers. Many financial services firms do not conduct within the same entity or affiliated entities all of the functions necessary to serve their customers. In this regard, it is important to distinguish between third-party service providers and third-party marketing partners. Third-party service providers provide what might be called logistical support to a financial firm, such as check printing, or collections, or any number of similar services. These entities function as an extension of the financial firm's infrastructure and, significantly, there is no distinction as to the privacy and security protections applicable to the financial firm and the third-party service provider.

For institutions of all sizes, it is possible to obtain virtually any service from an unaffiliated third-party provider. The service may be less costly and of an overall higher quality than the individual institution could provide for itself, depending on a variety of circumstances. For smaller organizations that do not have in-house expertise, outsourcing may be the only alternative. Loan servicing and data processing are examples of outsourced services, performed internally for the financial services firm. E-banking, call centers, and automated teller machines are common examples of third-party service providers that customers use in obtaining services from their financial service firms. Financial institutions are required by the GLB Act to have administrative, technical, and physical safeguards to insure the security and confidentiality of customer records and information. These protections are achieved by contractual protections, careful selection and monitoring of third-party servicers, and technology solutions.

Marketing Partners. Many financial services firms do not offer individually (*i.e.*, directly manufacture) all of the products or services that they offer to their customers. A firm may find it more efficient, and less costly to its customers to enter into an arrangement to offer the product(s) of joint marketing partners. For example, a holding company's subsidiary bank may provide mortgage products to its customers, but not offer mortgages on vacation homes outside its local market or mortgages with non-conventional terms or other features. In order to provide its customers with local convenience and a wider selection of products, the bank finds an outside partner to offer the desired products jointly. Or, a firm may determine that offering credit cards to its customers is not the most efficient use of its resources, but does not wish to send its credit card customers to a competitor. That firm may choose to make arrangements with a third party or joint marketer to offer credit cards under the firm name to the firm's customers. It appears that consumers are generally indifferent as to whether a product is produced by the firm or a third party. Certain types of insurance products are another example of joint marketing arrangements that benefit the customer as well the firms offering and producing the product. This arrangement is most important and beneficial to firms of all sizes, but particularly, as described in the "Third Party Service Providers" discussion above, to community banks and their customers. Significantly, the third party marketer is subject to the same protections for customer information and security as the financial firm itself.

Customer Satisfaction and Branding. Most Roundtable members devote significant resources to providing high quality products and services under a recognized national, regional, or local brand or name. Customers have specific expectations when dealing with such an organization. It does not matter to the consumer whether he or she is dealing with one or more affiliates of a company. Nor does the customer often realize that a service or product is being provided by separate affiliates under the same corporate identity umbrella, and any distinction, we believe, would be confusing to the customer. The customer expects the same quality of product and level of service whether he or she

buys two products from the same company or the same two products from separate, but affiliated companies. Similarly, a customer expects that jointly marketed products will be convenient, useful and desirable from a cost perspective. What the consumer cares about is the quality and price of the product, and the quality of the service, regardless of how the corporate entity chooses to deliver it.

The Existing Framework Protects Customers.

Title V of the GLB Act requires each financial institution to establish and implement an information security program that includes administrative, technical, and physical safeguards best suited to the institution's size, nature, and scope of its activities. The Roundtable and it's sister organization, The Technology Group for The Financial Services Roundtable, (BITS), continually search out the best practices for protecting our members' systems and their customers' valuable information. Improvements can and will continue to be made both in enhancing our members' security practices and procedures and in managing the ways in which information is integrated for the benefit of customers. We communicate with federal, state, and local law enforcement authorities, federal and state regulators, and customers. For instance, with the assistance of law enforcement authorities we are developing more sophisticated ways to enhance our ability to detect and prevent the crime of identity theft. In addition, the industry is devoting meaningful resources to assist the victims of identity theft.

Specific Responses

In accordance with the instructions in the Treasury Department's request for comment, the Roundtable's specific responses to questions are identified with the number and letter of the question to which the response relates. For convenience and clarity, Treasury's questions are restated in italics, with our response immediately following.

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

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

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

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.

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

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

Response to Question 1 a-e.

The type of information that is shared with affiliates or nonaffiliated third parties is dependent upon the purpose of the sharing, including the services being performed by the affiliates or nonaffiliated third party. Generally, the amount of information shared with marketing partners is considerably less than that shared with affiliates or service providers. There are no economic or other incentives to sharing more information with marketing partners than is absolutely necessary. The very diverse corporate structures of Roundtable members and the various ways in which they choose to serve their customers dictates how information is shared by financial firms with affiliated or nonaffiliated third parties. In all cases, this sharing is done under the strict requirements, including confidentiality and non-disclosure, of the GLB Act.

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

Response to Question 1 f.

Financial firms voluntarily place limits on the sharing of information with both affiliates and nonaffiliated third parties. They did so even prior to the enactment of the GLB Act. These limits generally apply to the function to be performed by the entity, not whether the entity is an affiliate or nonaffiliate of the financial firm. The information that is shared is limited to that which is needed to complete successfully the offering of the product or the providing of the customer service. Financial firms are highly motivated to protect information because they bear the direct financial loss of misappropriated customer information as well as the loss in customer confidence.

As noted in the Response to Question 1 a-e above, firms share significantly less information with marketing partners than with affiliates and service providers, because there is no benefit to the financial firm or its customers to sharing more information than necessary.

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

Response to Question 1 g.

There are generally no operational limitations that prevent or inhibit Roundtable members from sharing information with either affiliates or nonaffiliates. Any operational issues that may exist are likely to be unique to a given financial services firm.

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?

Response to Question 1 h.

The Roundtable believes that there must be a balance between information sharing and customer privacy. We believe that the GLB Act and its implementing federal regulations strike the appropriate balance and we believe that this balance should be the uniform national standard.

The Roundtable did not survey its membership with regard to whether there are other purposes for which our members would like to share information with affiliates and nonaffiliates but do not. Based on our survey and information from our members:

- Social security numbers are shared only for customer identification purposes;
- Medical data (other than as necessary for information processing) is not shared; and
- Information on specific credit card purchases is shared only for affinity cards, rewards, and similar programs, and not for what is generally considered traditional customer profiling or modeling.

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.

Response to Question 2 a.

As a preamble to the response, the specific answer is a moving target because the security protections used by our firms are a function of the complexity of the technology and systems used to integrate data and the security technology available to respond to the recognized need. The types of safeguards currently employed by financial firms are

extraordinarily numerous and improving constantly to incorporate technological advances.

As stated in the question, the types of security protections that financial firms have in place may be thought of as technical, administrative, and physical. Technical protections include techniques and mechanisms such as encrypting information internally, employing outsiders to break into systems to determine vulnerabilities, specialized tools to authenticate access to systems such as the use of a personal identification number, employing the developing device of biotechnology systems to enhance security, conditioning customer internet account access on the use of threshold levels of technology with built-in security protections (such as browsers with 128 BIT SSL capability), and many more kinds of protections.

Administrative protections would include, for example, precise segregation of duties to limit the scope of systems access, employee training, adherence to security and corporate ethics policies, background checks of employees that have access to sensitive information, and regular internal and external examinations. Extensive administrative protections are built into financial firms systems, including requiring a business purpose to share information and requiring an access code for access to certain types of information.

Physical protections would include, among other things, low visibility data centers with hardened parameters and restricted data center access with two factor authentication required for entry.

These protections and, as suggested, many others have been employed extensively by financial firms long before the passage of the GLB Act to protect and secure customer information.

As noted earlier in this document, the protections applicable to, and employed by, financial firms are imposed on all third-party service providers and marketing partners.

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)?

<u>Response to Question 2 b.</u>

The financial services industry recognizes the imperative to protect and safeguard customer information for two primary reasons. First, customers expect and demand safeguards as a condition of doing business with them. Second, customer information is a valuable asset for every firm and to give or sell that valuable asset, particularly to a possible competitor, makes little economic sense. As noted in the question, GLB requires

that every financial firm maintain adequate security measures, which are enforced by the state and federal functional regulators.

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

Response to Question 2 c.

Existing requirements wisely provide for future changes in available and needed security measures. As we noted at the beginning of the question, security measures will change as the technology in the marketplace changes. Flexibility is built into the GLB statutory system. Each new product and new technology opens new possibilities for hackers and thieves. The importance of flexibility so that the marketplace can respond to such threats cannot be overstated. The Roundtable believes that our members employ the best available security measures commensurate with the complexity of the systems used by each firm. The industry invests huge amounts in funds and intelligence in system resources in an ongoing effort to stay on top of ever-widening security requirements. In addition, those resources also are applied to the anticipation of issues that haven't yet arisen, but which will arise in the future.

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

Response to Question 2 d.

We have no additional protections to suggest at this time, except to urge strongly that the industry, the functional regulators, and federal, state, and local law enforcement authorities continue to share information about this issue. We would only make the point that it is in the industry's enormous self-interest to safeguard information. In this regard, we continue to make improvements in the ordinary course of our efforts to protect customer information.

Our responses to do not address any of the cyber-security or critical infrastructure issues.

Question 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?

Response to Question 3 a.

First, we believe that sharing of information with affiliates and nonaffiliated third parties actually reduces potential risks to customers by helping prevent fraud and identity theft. While information sharing always poses some degree of risk, we believe that this risk is more than balanced by the benefits to consumers.

Second, we do not believe that information sharing with an affiliate possesses any unique potential privacy risks to customers. Because affiliates are part of the same corporate structure, all affiliates are subject to the same control mechanisms for ensuring security of the information and confidentiality as the disclosing institution. The confidentiality obligations, as required by the GLB Act, are in place with regard to affiliates.

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?

Response to Question 3 b.

We believe that any risk that a customer might face from the disclosure of information to a nonaffiliated third party is mitigated by the financial institution's obligation to ensure strict security and confidentiality. It is the responsibility of the disclosing financial institution to:

- Assess the risks to the security and confidentiality of the information that the disclosure could create;
- Do appropriate due diligence regarding the third-party's information handling practices;
- Negotiate appropriate protection for the information before it is disclosed, including agreements to not use or disclose the information other than for the specified purpose, and to have an adequate information security program in place and to maintain it while the third party has the data.

Moreover, the adequacy of a financial institution's protections and security measures are subject to review and oversight by the state and federal regulators. Misbehavior by a third party usually leads to reputational damage and in this case would lead to a loss of business from financial institutions.

It is important to note that some disclosures are required by law, or to regulators, and, as such, would not be subject to the institution's ability to negotiate protections for the data.

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?

Response to Question 3 c.

All affiliates of a financial firm are subject to the internal controls of that parent firm with regard to information usage. We do not believe that interaffiliate sharing of information with a nonaffiliated third party poses any privacy risk different from a risk that exists with the direct sharing of information by the institution with the third party. See 3b above.

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

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

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

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

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

Response to Question 4 a - d.

There are no distinctions in benefits from information sharing based upon whether the entity sharing or receiving information is the financial institution, an affiliate, or a nonaffiliated third party. Financial firms and their affiliates benefit from a number of efficiencies that flow from information sharing. Information sharing permits financial firms to offer services as well as more products and services at lower costs to their customers. Efficiencies, in effect, get built into the system and customers benefit. For example, firms are in a better position to offer bundled services at reduced costs to their customers, which may also lead to discounts for certain services and products. Also, speed to market and claims processing are two of the benefits that flow from the increased efficiency resulting from information sharing.

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

Response to Question 4 e.

As reported in our attached Survey, information sharing helps prevent fraud and identity theft. These crimes result in increased costs of operation for firms and their affiliates, which also result in increased costs of products and services to customers. Illustrative of the costs of restrictions on sharing and the benefits of the current system is the type of phone call that is made thousands of times every day. Ms. Jones, holder of an X brand credit card, receives a call from a person in a credit card call center, located in a midwestern state, who is employed by Ms. Jones' credit card company, which is located in a southern state. The caller alerts Ms. Jones that her card has been used to purchase a mink coat in New York City and asks if she in fact made the purchase. Ms. Jones, residing on a farm in Vermont, denies the purchase. The card company tries to stop the transaction, voids her card account, and sends her a new card with a new number, hassle-free to Ms. Jones.

Consider the chaos if states, with good intentions, limit the flow of information or if customers nationwide can prevent the sharing of critical information. Extrapolate that routine example into the number of ways that humans can think of to commit fraud and the potential damage to the financial system and consumers can be better appreciated.

Information sharing accomplishes much more than helping prevent fraud. There are numerous benefits resulting from information sharing as discussed in the Response to Question 5. Thus, an exemption for sharing information solely for fraud prevention, unfortunately, is not the solution. The harm would be to reduce consumer benefits and reduce the availability of the lower cost of credit, among others.

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

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

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

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

Response to Question 5 a-c.

In addition to the benefits identified in our Survey and as detailed more fully below, information sharing and its resulting transparency in the credit granting process

increase the availability of credit to the market in general and reduce the cost of credit to the customer. In Europe, for example, financial information sharing is more limited than in the U.S. Consequently, mortgage rates may be as much as two percentage points lower in the U.S. than in Europe. (See Kitchenman 1999 referenced above and in the Survey). Lower rates mean more consumers qualify for loans. In addition, consumer credit decisions are made within hours, if not immediately, in the U.S., as opposed to taking weeks or months in Europe. And it only makes sense that the more information that a potential lender knows about a customer, the easier it is to price the risk and make a loan to that customer. This may be one of the explanations of why so many more individuals have access to credit in the U.S.

Because of the varied ways in which Roundtable members and other financial service firms offer products and services to customers, specific customer benefits flowing to consumers from sharing information with or between affiliates and with nonaffiliated third parties are identifiable and quantifiable. In certain instances, the Roundtable Survey provides estimations of the benefits, although overall, we believe an assessment using such distinctions would not be particularly useful given the variety of ways financial firms operate. Thus, our discussion focuses on aggregate benefits to customers of information sharing, regardless of the entity receiving the information.

Customers of financial services companies obtain significant benefits from information sharing, including increased convenience, personalized service, fraud detection and prevention, and real savings of time and money. The information sharing provides customers with more services at lower prices, and allows the companies to increase efficiency, lower costs, and pass those savings on to customers. The Roundtable survey estimated the benefits to customers of the 100 largest banks, insurance, and securities companies that are members of the Roundtable. Based on publicly available industry data and a survey of the membership, the findings are:

- Savings Per Household. Information sharing saves Roundtable members' customers, on average, $195 per customer household per year. In addition, the average household saves close to four hours per year due to the convenience provided by information sharing.

- Money Saved. For all customers of the Roundtable's members, the total dollar savings due to information sharing is about $17 billion per year. About $9 billion of this total comes from information sharing with third parties, and about $8 billion comes from information sharing with affiliates. These estimates would be larger for the entire financial services industry.

- Time Saved. Information sharing saves Roundtable members' customers about 320 million hours per year. About 115 million hours are saved because of

information sharing with affiliates, and 205 million hours are saved because of information sharing with third parties.

- Types of Benefits. Customers benefit from information sharing across a wide variety of services. They save money from outsourcing to third parties, relationship pricing, and proactive offers. Customers save time because of information sharing by call centers, internet based services, third party services, proactive offers, and pre-filled applications.

- Mass Marketing versus Targeted Marketing. Privacy concerns are partly motivated by marketing solicitations. Contrary to common perception, however, the ability to share information can actually reduce the number of solicitations consumers receive. The Roundtable members save about $1 billion per year by using targeted marketing instead of mass marketing – savings which can be passed forward to customers. A shift back to mass marketing could force companies to send out over three times as many solicitations to achieve the same level of sales.

Additional examples of information sharing benefits from our Survey include:

- A large share of the time and money that is saved is from third party services, a subset of all benefits from sharing with third parties. Many financial services providers are seeking to provide "one-stop shopping" through a full range of financial services, and are partnering with third parties to provide their customers with low-cost, efficient services (e.g., credit cards, insurance). Using third parties allows financial institutions to provide additional services to their customers more efficiently and less expensively than if they had built the same service lines in-house, saving customers about 170 million hours a year and $7 billion annually.

- Call centers provide significant savings of time. Companies integrate their call centers for different affiliates and/or third parties to allow customers the ability to access all their accounts with one phone call. Internet based services, which provide similar convenience, are still a relatively new but rapidly growing delivery channel. Call centers save about 70 million hours and Internet based services save over 30 million hours a year.

- Proactive offers and relationship pricing provide significant savings of time and money for Roundtable member customers. Proactive offers save customers time (50 million hours) and money ($7 billion) by offering and educating them about services when they are most likely to need them, for instance, offering a customer lower premiums on automobile insurance because of improvements in her driving record. Relationship pricing allows financial institutions to provide lower prices for customers with multiple relationships spanning different affiliates or third parties, saving customers over $2 billion a year.

These information sharing benefits only account for the savings provided by the 100 member companies of the Roundtable. It does not include savings created by information sharing at thousands of other U.S. banks, insurance firms, securities companies, thrifts, and credit unions.

Importantly, these information sharing benefits do not include:

- Savings from fraud reduction;
- Customer benefits from the expanded availability and lower price of credit due to better risk quantification;
- Benefits from ATMs and co-branded or affinity credit cards; and
- Future benefits derived from information sharing.

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

Response to Question 5 d.

The Roundtable is not aware of any reasonable alternatives that would provide the same or similar benefits for customers while at the same time protecting the confidentiality of customer information.

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

Response to question 5 e.

The benefits to customers described in the Response to Question 5c are significant. Information sharing provides real benefits to customers. Further limitations on the sharing of information would result in reducing each of the benefits described above. If additional restrictions were placed on the sharing of such information with affiliates and third parties, these benefits to customers – at least $17 billion of cost savings and 320 million hours of time savings annually – would be at risk. A negative impact of this magnitude merits serious consideration before any additional restrictions are placed on information sharing by financial services companies.

Question 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.

Response to Question 6 a.

The existing laws provide adequate protections for customer privacy. Title V of the GLB Act establishes, for the first time, a federal law governing a financial institution's use of customer information; it does not supplant other privacy protections, such as the Electronic Fund Transfer Act, the Right to Financial Privacy Act, or most importantly, the Fair Credit Reporting Act. The opt-out feature of the GLB Act, which generally affords customers the opportunity to prevent information from being shared with nonaffiliated third parties for marketing purposes strikes, in our view, the appropriate balance between protecting customer privacy and permitting the sharing of information by financial institutions. This balance produces benefits that are achieved through efficiency in operations and passed on to customers in the form of greater availability of credit at lower costs and enhanced services. The Fair Credit Reporting Act strikes a similar balance, one that the Roundtable believes is appropriate. Both statutes establish a national uniform standard in requiring disclosures on privacy protection. Unlike the Fair Credit Reporting Act, however, the GLB Act permits some individual states to enact different customer protections, which add confusion for customers' understanding of their rights and compliance responsibilities for financial institutions.

We believe that a patchwork of state laws with differing requirements and different levels of protections reduce the benefits that have been demonstrated above. (See Response to Question 5). Such a set of differing requirements would significantly add to the confusion of customers' understanding of their rights. A patchwork of different state laws would add to the compliance responsibilities of financial institutions and add to the costs of providing products and services to customers. Such increased costs to financial services firms results in increased costs to customers or reduced benefits.

The GLB Act is less than three years old and the final regulations are one year old. Experience to date has not produced any significant deficiencies in the privacy protections it affords customers. It should be given a fair chance to operate before changes make it impossible to assess.

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

Response to Question 6 b.

The Roundtable believes that a uniform national standard should be made a permanent part of the GLB Act, as it was for seven years under the Fair Credit Reporting Act. We recognize that such uniformity is set to expire under the Fair Credit Report Act on December 31, 2003, and we strongly endorse making that permanent as well. There is no question that multiple, additional state restrictions will be chaotic for both consumers

and financial institutions. The uniform system has worked well under the Fair Credit Reporting Act and should be embraced for the GLB Act. Otherwise, the real benefits of a uniform national information sharing regimen will be significantly diminished.

The insurance industry poses unique problems because it is a state regulated industry. Therefore, in order to provide the necessary authority for the "functional regulator" to enforce the GLB Act, each state needed to enact legislation or adopt a regulation. Many states ultimately adopted the model regulation published by the National Association of Insurance Commissioners, but there still are differences state by state, including some states with no legal requirements, and some with conflicting requirements. As a result, there is not the kind of national uniformity that we have in other financial services industries. The privacy protections for insurance customers need to be uniform, and they need to be the same as the protections for customers of other financial services businesses. This again, argues for the establishment of a uniform national standard.

The Roundtable and its members recognize that identity theft is a significant issue, but we believe that this issue should be addressed separately from information sharing; it is a very real problem that deserves scrutiny and action. Identity theft is an issue of criminal conduct on the part of individuals, not financial institutions, and has little to do with the core privacy issue of information sharing. Indeed, as demonstrated in our Study, information sharing actually assists in reducing both identity theft and fraud.

Question 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.

Response to Question 7 a.

Our comments on this question are limited to the requirements of Title V of the GLB Act. In this regard, we believe that financial institution privacy notices have been adequate under the existing law, but they also have been somewhat complex and legalistic.

The disclosure requirements of the GLB Act were new to consumers, financial institutions, and their regulators on July 1, 2001. In order to comply with these new requirements, financial institutions worked with their regulators to satisfy the disclosure requirements. The complex nature of the disclosure was compounded by the uncertainties of potential liability for failure to disclose all that was involved under the broadly worded statutory requirements. The disclosures were necessarily detailed because of the complex statutory framework. The process resulted in perhaps more thoroughness

than clarity. Efforts are ongoing between the industry and regulators to make the notices more user friendly.

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.

Response to Question 7 b

We believe that in the future, notices could be made shorter, more easily understandable, and overall, more meaningful. A more user-friendly privacy notice would produce greater customer benefits through greater understanding of what is involved and increase the level of trust between financial institutions and their customers.

We note that the annual notices are costly to provide and of questionable utility to customers. We suggest that establishing a better balance between informing customers adequately and clearly, on the one hand, and the annual costs involved in doing so, on the other, would be helpful to both customers and financial firms.

In addition, there is some ambiguity in the "annual" requirement and whether a calendar year disclosure will satisfy the statute's requirements. These issues could be addressed by the regulators.

Question 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.

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.)

c. Is it feasible to require financial institutions to permit customers to opt out generally of having their information shared with affiliates?* (*This question seeks views on a general opt out for sharing of information with affiliates and represents a broadening of opt-out provisions for affiliate sharing under the FCRA. Please explain what effects, both positive and negative, such a requirement would have on consumers and on financial institutions).

Based upon the experience all financial institutions have had with the GLB Act, current estimates are that only two to five percent of all customers opt-out of information sharing with unaffiliated parties, as permitted under the statute. This indicates to us that the overwhelming majority of consumers are satisfied with the status quo. In other words, almost all customers appear to be comfortable with allowing their financial institution to continue to share information as their company was doing before the passage of the GLB Act, and beyond what is authorized by the GLB Act. In addition, the consequences of more restrictions on information sharing are difficult, if not impossible, to predict. Some products and services are not capable of being marketed with an opt in requirement To some extent, the answer would depend on the particular financial institution involved. Moreover, a mixed system of opting in for some products or services would require an integrated data information system that is not currently available. In any event, an opt-in requirement for some or all aspects of the financial services industry would produce less competition and higher prices for consumers.

<u>Response to Question 8 a-c</u>.

Questions 8 a through c ask about, among other things, the feasibility of requiring affirmative consent, or "opt in", in order to share information with affiliates and third parties. We have assumed for purposes of our response to these questions that the "sharing" inquired about was for purposes of marketing products or services to customers, but for many organizations, data sharing for a wide variety of operational purposes is necessary to their ability to do business.

In any organization that does not contain all operational functions within its corporate walls, information may have to be provided to affiliates or third parties so that the disclosing institution can provide services to customers, or receive services necessary to operate its own business. For example, a financial institution that is a member of a financial firm may obtain loan processing services from an affiliate, and the affiliate may require access to information about customers to provide the service. Similarly, information technology hardware may be owned or provided by an affiliate, such that a financial institution uses hardware owned by an affiliate, serviced by the affiliates and a variety of third-party service providers with specific expertise, and for which software is developed and maintained by still another group of affiliates and third-party providers. Access to customer information may be required to perform all these functions in the

ordinary course of business. In the interest of brevity, we have provided only these two examples, but there are many similar business circumstances. In addition, disclosures to regulators for regulatory oversight require the sharing of data.

The GLB Act recognized the need for these types of day-to-day operational access to personally identifiable information, and specifically provided that in nearly all instances those disclosures are not subject to either notice or customer right to opt-out. Simply stated, these kinds of information sharing are essential to daily business functions.

On the issue of disclosure of medical information, the insurance industry practice is to obtain customer's consent before disclosing medical information. In fact, the "NAIC Model of Privacy of Consumer Financial and Health Information Regulation," adopted in over 40 states, imposes such a requirement. Therefore, as long as any rules include the essential exceptions for those business functions described in the GLB Act's Section 502(e), we would support a prohibition on the disclosure of health information for marketing products and services.

With regard to the feasibility of customers opting in to information sharing with affiliates, we believe such a provision that is beyond the customer choice already provided in the Fair Credit Reporting Act would require massive changes to firm operations. Requiring multiple processing capabilities for firms will simply be cost prohibitive for many firms, inhibit the ability of firms to respond to customer complaints, and force choices on firms that will harm consumers.

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.

<u>Response to Question 8 d.</u>

Aside from the medical information sharing discussion above (see Response to Question 8 a - c), the Roundtable believes that it is not appropriate to have customers generally opt-out of information sharing with affiliates or nonaffiliated third parties, or across business lines, nor are we aware of any alternative methods that would generate the same level of benefits to customers while protecting the privacy of customer information.

For example, fraud and identity theft cost Americans more than $37 billion each year. Victims of identity theft spend an average of 175 hours and $800 to rectify the damage (CALPIRG/Privacy Rights Clearinghouse, 2000). Shared information enhances the detection and prevention of such frauds.

Another benefit of information sharing is the availability of credit at lower cost. In Europe, financial information sharing is significantly limited. As a result, U.S. mortgage rates are typically two percentage points lower than in Europe (Kitchenman, 2000).

Question 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?

Response to Question 9 a.

With the exception of possible limits for the sharing of medical information (see Responses to Question 8 above), the Roundtable believes that restricting the sharing of information for specific uses or directing the specific uses for which the information could be shared are generally unworkable if customers are to continue to maintain the benefits they currently enjoy. We strongly believe that allowing a customer to direct the sharing of information that is inconsistent with a firm's privacy policy would be damaging. As an example, customer service representatives should not have the authority to accept individual attempts to change a financial institutions privacy policy, the implications of which neither the employee nor many customers' fully understand. Also, permitting customers to direct how information is shared would, in effect, preclude financial institutions from having transactions processed by third parties. Financial firms could not operate in such an environment.

Allowing a customer to opt-out of information sharing for specific purposes runs afoul of the multiple database dilemma—multiple databases would be cost prohibitive for many firms and force choices on firms that would only damage a consumer, not add value to the consumer's relationship with a financial institution. Multiple processing mechanisms increase the inefficiencies of financial firms, reduce consumer benefits and possibly impair financial firms ability to accurately respond to governmental requests for information about criminals.

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

Response to Question 9 b.

The Roundtable believes that restricting the sharing of information to specific or directed uses would make it:

1. more confusing to consumers,
2. more costly to administer,
3. more costly to obtain products and services, and
4. more likely to increase fraud and identity theft.

In short, it would force organizational, systemic and structural changes on financial institutions at enormous cost to the institutions and their customers.

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

Response to Question 9 c.

The Roundtable members have had no experience with allowing customers to restrict or direct the sharing of information by financial firms to particular uses.