28

Bank of America

Corporate Marketing & Communications
NC1-022-15-15
101 N. Tryon St.
Charlotte, NC 28255

Tel 704.386.9643
Fax 704.388.9162

VIA ELECTRONIC DELIVERY – study.comments@ots.treas.gov

April 30, 2002

Regulations and Legislation Division
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, NW
Washington, DC20552

Attn: Study of GLBA

Re: Comments on GLBA Information Sharing Study

Ladies and Gentlemen:

Bank of America is pleased to submit these comments in response to the Department of the Treasury's request, pursuant to section 508 of the Gramm-Leach-Bliley Act (the GLBA), for comments on information sharing practices among financial institutions and their affiliates. Bank of America is one of the world's leading financial services companies, and is the sole shareholder of Bank of America, N.A., one of the largest banks in the United States. Through the nation's largest financial services network, Bank of America provides financial products and services to 30 million households and two million businesses, as well as providing international corporate financial services for clients around the world.

Bank of America was the first major financial institution to announce, in June 1999, that it was adopting a policy of not sharing consumer customer information with nonaffiliated companies for purposes of marketing their own products and services. We have been very forthright, however, in letting our customers and others know that we do manage customer information among our affiliates in order to meet our customers' expectations with regard to the delivery of financial services.

We recognize that it is not, and should not be, our customers' responsibility to understand how we have chosen to organize our company into various legal entities for legal,

regulatory, financial or other reasons. We know that our customers view Bank of America as a single enterprise and that they expect us to deliver financial services to them as a single enterprise, regardless of the location or channel through which they choose to communicate with us at any particular time. In fact, significant portions of the technology and other strategic investments Bank of America has made within the last decade have been focused on that very objective -- to make Bank of America more responsive to our customers' expectations that we make it even easier for them to obtain the full range of customer service and financial services at every point through which they might choose to access us: by phone, through a banking center, through their personal computer. We know that a leading reason that former customers have terminated their relationships with us is that we have not always been as effective as we can be in managing customer information across our affiliates in a way that enables us to resolve customers' problems quickly, show that we recognize and value the customers' total relationship with us or effectively anticipate our customers' needs. We know, because our customers have told us, that the key to satisfying them is to make customer information readily accessible to (in other words, to share information with) our employees who interact with customers so that they have the information and tools to serve customers and solve their problems.

We are pleased that the Secretary of the Treasury, in conjunction with the federal functional regulatory agencies and the Federal Trade Commission, is conducting a study of the sharing practices among financial institutions and their affiliates. We believe that a review of the practices will show that affiliate sharing practices have a single objective: to deliver the quality of financial services that consumers have been craving for many years and to make available to the average consumer the kinds of service that heretofore has been available only to the wealthiest financial services customers.

The attached document responds to specific questions posed by the request for comments. Thank you for this opportunity to provide information regarding our practices.

Sincerely,

Robin K. Warren

Robin K. Warren
Privacy Executive

GLBA Information Sharing Comments of Bank of America

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 non-affiliated 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:

As indicated in our Privacy Policy for Consumers, Bank of America shares the following types of information among the Bank of America subsidiaries that provide products and services to consumers or that perform operational support for those products and services:

1. Application Information -- information, such as a customer's assets, income and debt, which a customer provides to us on applications and through other means.
2. Transaction and Experience Information — information about a customer's transactions and account experience, such as account balances, payment history, parties to transactions and credit card usage; or information about our communications to our customers, such as requests for copies of checks and our responses, or pre-approved credit card offers.
3. Consumer Report Information — information from a consumer report, such as a customer's creditworthiness or credit history.
4. Information from Outside Sources — information from outside sources regarding their employment, credit and other relationships with our customers or verifying representations made by our customers, such as their employment history, loan balances, credit card balances and their property insurance coverage.
5. Other General Information — information, such as demographics, that is not assembled or used for the purpose of determining a customer's eligibility for a product or service.

We know that most of our customers think of Bank of America as one company, rather than as a family of companies that provide a variety of financial services. That's why the sharing of customer information among affiliates is critical to meeting customers' service expectations. For those customers and others who want specific information about the affiliates with whom customer information is shared, a complete list is appended to the Privacy Policy posted at our website: http://www.bankofamerica.com/privacy

Bank of America does not sell or share customer information with marketers outside Bank of America for purposes of enabling those nonaffiliated parties to market their own

products and services. Customers do not have to tell us not to; we will not do it and have not done so since 1999. In addition, we do not provide customer information pursuant to joint marketing agreements with other financial institutions unless we have customer consent to do so.

We do make customers aware of offers from businesses we work with, if we believe they have a product or service that might interest an individual customer. But we do not provide these companies information about a customer. We leave that decision up to the individual customer.

Additionally, we furnish customer information to nonaffiliated third parties that provide services on behalf of Bank of America. All such service providers are contractually obligated to keep the information we provide to them confidential and secure, and to use the customer information we share only to provide the services we ask them to perform for our customers and us. Examples of nonaffiliated third party service providers include payment processing companies, check printers and data processing companies.

Customer information is also shared with nonaffiliated third parties pursuant to the exceptions under Section 502(e) of Title V of the Gramm-Leach-Bliley Act (GLBA). For example, information is furnished: to consumer reporting agencies; to governmental agencies in conformity with the provisions of the Right to Financial Privacy Act and the USA PATRIOT Act; in connection with asset securitizations; as necessary to effect, administer and enforce transactions with our customers; to protect against fraud; pursuant to legal process, such as subpoenas.

Information is shared with affiliates to facilitate customer service, to detect and prevent fraud and unauthorized use of accounts, to facilitate research and analysis of aggregate customer data, and to appropriately target our marketing efforts. In order to improve our ability to respond to customer inquiries regardless of the location or communications channel through which the customer chooses to contact us, we are investing much of our systems development resources into enhancing our systems for centrally managing our customers' information. The centralized management of customer information across our enterprise has a variety of benefits that our customers tell us they expect from us. Centralized management of information:

1. Enables customers to get account information, including balances, payoffs, transaction details, at all customer contact points, including our banking centers, telephone customer service centers, and through our online banking service.
2. Allows expedited processing of loan applications and other account applications because the customer does not need to re-furnish information he has previously furnished to Bank of America.
3. Allows customers to link accounts in order to obtain overdraft protection on their checking accounts or to avoid other service charges.
4. Enables tellers to make more of our customers' deposits immediately available to the customers.

5. Helps us to tailor information about our products and services to a customer's unique needs rather than pushing services that the customer already has or that the customer has no need for.
6. Enables all of our sales and customer service associates to see and honor customer preferences with regard to receiving direct marketing via telephone, U.S. mail or e-mail.
7. Allows us to offer customers discounts and/or additional services based on the value of their total relationship.

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

Response:
Bank of America does not sell or otherwise share customer information with nonaffiliated third parties for purposes of marketing their own products or services.

Bank of America does not share medical or health information among its affiliates, except as necessary to maintain accounts, process transactions, service customer requests or perform insurance functions on a customer's behalf.

Bank of America affords its customers the choice not to receive marketing offers from us by direct mail, telephone and/or e-mail. Regardless of how, when or where a customer notifies us of his direct marketing preferences, those preferences are honored across the enterprise by all affiliates. That means, for example, that if a credit card customer has chosen not to receive telemarketing calls from Bank of America, neither our credit card affiliate nor the bank may use information about the customer's credit card account for purposes of contacting the customer by telephone to offer another service, such as a checking account or a loan. In addition, to minimize the amount of telephone solicitation our customers receive, we do not offer non-financial products or services through telemarketing.

2. *The extent and adequacy of security procedures 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:
Bank of America Board of Directors has approved a Corporate Information Security Policy and Program designed to protect and safeguard customer and corporate information and information system resources. Access to customer information is made only to the extent necessary to provide products and services or to maintain those products and services. All associates are bound by a code of ethics requiring confidential treatment of customer information and associates are subject to disciplinary action if they fail to follow this code. Bank of America associates are required to understand and to take action to ensure compliance with any and all specific policies, procedures, standards and guidelines established in support of the Corporate Information Security Policy.

Bank of America employs an array of procedural and technical controls to manage and administer authorized access to various information resources and information across the family of Bank America companies. Additionally, various technologies, procedures and monitoring are deployed to protect against, detect and to prevent attempts to gain unauthorized access to networks, systems and information resources. Complemented by a physical security program that provides protective measures to control physical access to sensitive facilities and processing areas, keeping financial information secure is one of our most important responsibilities. Procedures are in place to protect all forms of information, whether it is in electronic or paper form, as well as to insure critical information is backed up and available to ensure continuity of operations. Finally, when information or information systems that contained sensitive or confidential information are no longer required, appropriate disposal procedures are designed to maintain the confidentiality of information.

We continually assess new technology for protecting information and upgrade our systems when appropriate.

When contracting with third party service providers, contract requirements are established to ensure confidentiality and compliance with regulatory requirements for the privacy and safeguarding of customer information. Bank of America by contract requirements reserves the right to conduct audits and reviews of the privacy and security practices of our service providers.

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)?*

Response:

The safeguards employed are consistent with existing law. The processes established under the Interagency Guidelines for Safeguarding Customer Information, described in 12 CFR 30, Appendix B, provides a comprehensive approach and practice for making the appropriate assessments and allows the risks to be managed and appropriate controls implemented consistent with the sensitivity and risks to the information and information systems. Additionally, oversight and reporting requirements in the guidelines provide regular management opportunity to monitor the Corporate Information Security Program and to make appropriate adjustments to the program.

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

Response:

The existing statutory and regulatory requirements provide sufficient flexibility for institutions to establish and adjust appropriate protective procedures and controls to protect information consistent with the risks and sensitivity of such information, new business services, new delivery channels, and the use of new technology for delivering such services. Regulatory guidelines that focus on assuring "good processes and decision making" is followed verses ones which would provide rigid and specific mandates allows institutions to effectively and efficiently establish the appropriate and necessary controls for safeguarding information consistent with the individual institution's unique

environment, service offerings, and the risks and the sensitivity of information being managed and processed. Both internal and examiner audits and reviews provide the mechanisms for ensuring the intended processes guidelines are appropriately followed and implemented.

3. *The potential risk 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 affiliates?*

Response:
Although we are not aware of any risks to a customer if information is shared among our affiliates, we know that there are risks to our customers if information is not shared. The risks range from economic harm to inconvenience. Risks that our customers face if we do not share information across our enterprise include:

- Increased risk that fraud or other unauthorized activity involving multiple accounts will not be detected
- Increased risk that their deposits will be subjected to unnecessary holds
- The risk that the credit card payment they make at a banking center or at an ATM will not be transferred to their credit card account in sufficient time to avoid a late charge.
- The risk that all Bank of America affiliates will not know and, therefore, will not honor, their direct marketing preferences.
- The risk that one call to our customer service center to report a stolen wallet will not suffice to as notice regarding the loss of credit, as well as debit cards.

Of course, all of our affiliates are subject to the requirements of the Bank of America Privacy Policy for Consumers. Their receipt, use and protection of customer information in conformity with our Privacy Policy is also subject to regulatory oversight by the financial institution supervisory agencies with jurisdiction over their activities, including the Office of the Comptroller of the Currency, the Securities and Exchange Commission, the Federal Reserve and various state insurance regulators.

4. *The potential benefits for financial institutions and affiliates of such sharing of information:*
    a. *In what ways do financial institutions benefit from sharing information with affiliates?*

Response:
The primary benefit to Bank of America is that the sharing of information helps us to increase customer satisfaction. Dissatisfied customers tell us that the chief reason they are dissatisfied is because they had a problem that we were not able to resolve with one phone call. And the major reason that problem resolution takes more than one call is because customer service associates do not have access to all the information, including affiliate information, they need to resolve customers' problems.

Bank of America has made no secret of its objective: To convince our customers that they want to continue doing business with us and that they want to do even more business

with us. Time and again, customers have told us that the way to achieve that objective is to manage customer information across the enterprise in order to provide service and financial solutions to them whenever, wherever and however they find it most convenient to interact with Bank of America. When our customers benefit from the sharing of information with affiliates, Bank of America benefits, too.

5. *The potential benefits for customers of such sharing of information:*
    a. *In what ways does a customer benefit from the sharing of such information by a financial institution with its affiliates?*
    e. *What effects, positive or negative, would further limitations on the sharing of such information have on customers?*

Response:
There is only one way we can know our customers and help them get the service and benefits they want and deserve, and that is to function as one company by managing information across the company. We manage information about our customers across the boundaries of our various lines of business, such as credit card, mortgage, as well as our consumer, commercial and corporate banking units, and this also allows us to answer their questions, understand their needs and offer them the best potential solutions.

This not only helps us give customers better service and provide them more convenience, it also lets us offer them benefits based on their overall business with us, such as providing us with the ability to alert a customer who has several different accounts with us that she qualifies for an Advantage Account. By signing up for Advantage, this customer can avoid monthly fees for checking, get free banking services including free checks, free second checking account, free savings accounts and other no fee services such as a safe deposit box, cashiers checks, travelers' checks and stop payments, as well as preferred rates on loans and deposits. And she receives all of these benefits without incurring any new cost. The savings to an Advantage account customer can be as much as $669 or more annually.

Managing information centrally also lets us see unusual activity and variations – a powerful tool to protect our customers from fraud and identity theft and to help victims recover. For example, we may use information about a customer's ATM, credit card and check card transactions to identify any unusual activity, and then contact that customer to determine if their card has been lost or stolen.

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?*

Response:
As FTC Chairman Muris noted recently, consumer privacy concerns generally fall into 3 categories: (1) concerns about physical security; (2) concerns about economic injury, specifically the injuries caused by identity theft; and (3) concerns about unwanted intrusions.

As to the first type of concern, financial institutions and the companies we do business with have a long history of protecting the physical security and confidentiality of confidential financial information. The safeguards required by GLBA have served to ensure that every financial institution places a renewed focus on information security. Recent events have made it all too clear that it is crucial to public safety that all financial institutions have procedures in place to identify and authenticate the identity of those who do business with us. We are mindful of the important role we play in helping our government to identify and apprehend those who would do harm to the American people, be it physical or economic harm. The USA PATRIOT Act gives government agencies the ability and financial institutions the obligation to report information that may be relevant to suspected terrorism.

With respect to the second set of concerns, consumer reporting agencies, credit-granters, and others are developing increasingly sophisticated tools to detect and prevent fraud and identity theft. Recent reports have highlighted identity theft as the fastest growing crime in America. There are many reasons why identity theft is on the rise. Certainly one reason is the easy access to information, including information that wily identity thieves and their accomplices induce consumers to divulge unwittingly. Another reason that identity theft is growing is simply because it is so easy for the crooks to get away with it. It is difficult for law enforcement agencies to trace the perpetrators of this crime and, even when the ID thieves are identified, it can be extremely difficult to prosecute them. The crime typically crosses many legal jurisdictions and law enforcement across municipal and state boundaries presents a unique set of challenges. Today, identity theft is both profitable and low risk to the criminals who prey on consumers and the businesses that tally increasingly greater fraud losses each year. The surest way to bring identity theft under control is to implement effective methods to bring the thieves to justice.

As for the third concern, consumers have increasingly focused their concerns on telemarketing calls. Over 20 states have addressed this issue with "do not call" legislation. The Telephone Consumer Protection Act (TCPA) also affords protections to all consumers. And the FTC has recently proposed to establish a national "do not call" list pursuant to its authority under the TCPA. The Direct Marketing Association has established a national "do not call" list to which most [reputable] marketers subscribe voluntarily. And, like Bank of America, a growing list of companies have found that it is just plain good customer service to afford their customers the option to not receive telemarketing calls.

In addition to the security concerns, the issues surrounding privacy of consumer financial information reflect consumers' interest in knowing that confidential, sensitive information about their financial status and transactions will remain confidential. GLBA and the FCRA are adequate to protect the confidentiality of consumer financial information maintained by financial institutions. Like other financial institutions, Bank of America affiliates are subject to periodic examinations for compliance with FCRA and the privacy provisions of GLBA by their functional regulators. The FCRA provides appropriate restrictions on the release and use of sensitive credit-related information. Consumer reporting agencies that collect sensitive credit-related information are

restricted from disclosing it except to parties that have one of the specified permissible purposes. In addition, the FCRA also addresses disclosures of sensitive credit-related information among affiliated companies. It gives consumers control over whether affiliated companies can share this credit-related information by requiring the entity to notify consumers that it might be shared and providing them with an ongoing opportunity to prevent such sharing. FCRA also ensures that consumers are informed if financial institutions and their affiliates deny services to a consumer based on information contained in a consumer report.

GLBA restricts disclosure to nonaffiliated third parties of nonpublic personal information by financial institutions (which covers a broad spectrum of entities). Under GLBA, financial institutions cannot disclose nonpublic personal information (virtually all customer information held by a financial institution, including the fact that the consumer is a customer of the institution) to nonaffiliated third parties unless they have first provided notice to the consumer that they may do so and provided the consumer with an opportunity to opt out of such disclosures. The mandated notice must also be accompanied by the institution's full privacy policy addressing many information collection and disclosure practices. Thus, the consumer will have been provided with full notice of the practices of the institution and the intention to share and have the opportunity to prevent such sharing.

While GLBA only restricts disclosures of nonpublic personal information to nonaffiliated third parties, no further restrictions are needed for disclosures to affiliates. Generally, within a financial services company, a customer expects that the affiliated businesses will be familiar with the customer's entire relationship with the company and will recognize the customer's entire relationship appropriately in considering new products and offerings. Customers do not understand, and should not have the burden of determining, the complex legal structures of financial services companies that may be based on legal, regulatory or tax reasons. In addition, affiliated companies must be able to aggregate information about their customers in order to provide competitive product offerings and pricing, appropriate fraud protection and meet other legal and regulatory requirements such as compliance with the USA Patriot Act and anti-money laundering laws.

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

Response:

As stated above, much of consumers' concerns about privacy relate to receipt of unsolicited marketing, especially telemarketing. While there is quite a bit of legislation and regulation affecting telemarketing, there is currently no law that requires marketers to give consumers the option to opt out of receiving direct mail or e-mail marketing communications.

In addition, with respect to telemarketing, one national do-not-call list would provide one source for consumers to opt out of telemarketing and is preferable to multiple state lists with different requirements and different information. While the FTC has proposed to

adopt a national do-not-call list, it is not clear that the FTC would have the authority to preempt state laws imposing those lists. Bank of America is not opposed to "do-not-call" lists, and, in fact, has chosen to comply even when there are exemptions applicable to its calls. However, the many state laws establishing these lists contain different standards, exceptions and timing requirements and it is difficult to ensure compliance with multiple, different rules in a business with nationwide scope. In addition, consumers receive different treatment and protections in different states, even though many consumers are mobile and may move frequently. Therefore, we would suggest that legislation to create a national do-not-call list that would preempt state laws creating those lists would result in consumers' having better and consistent choices about receipt of telemarketing calls. Any such law should include an exemption for calls made to consumers with whom the company on whose behalf the calls are made has an established business relationship.

Another area that may require new statutory protection or, more likely, increased governmental resources, is in the detection and prosecution of identity theft. No matter how vigilant consumers and businesses are, identity theft will continue to grow until the criminals who engage in these activities see that they risk getting caught, convicted and imprisoned.

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?*
    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?*

Response:
New or revised disclosure requirements would not be helpful at this time. Though there has been much criticism of GLBA privacy notices, the fact is that the process envisioned by Congress is working. There is no doubt that financial institutions are working their way up the learning curve when it comes to communicating with their customers about their privacy policies. Consumers are also learning that different financial institutions have different privacy policies and they are learning that it is important to read not only their financial institutions' privacy policies, but also the privacy policies of other companies with which they do business. Consumers are learning to look for and read the privacy policies of companies whose websites they visit and to which they provide personal information.

The privacy notice requirements of GLBA are complicated. The law requires that financial institutions disclose to consumers the information that legislators and others thought consumers should know, not necessarily the information that consumers want to know. The law and implementing regulations also make it difficult to disclose information in a clear and direct way. For example, GLBA requires that consumers be given notice and the right to opt out of sharing information with nonaffiliated third parties. But that opt out right is subject to many legitimate and necessary exceptions. In fact, the primary sharing to which the opt-out right applies is sharing for marketing

purposes. Although it is good for consumers to know that information is furnished to nonaffiliated parties for a variety of purposes in the normal course of business, the listing of those exceptions in financial institutions' privacy notices creates confusion and constitutes information overload for many consumers.

Bank of America believes that it would be premature to revise the law or the regulatory requirements pertaining to financial institution privacy notices at this time. All of the parties involved in the GLBA privacy notices – financial institutions, regulators, advocacy groups, the media -- are learning from our experiences. Many of the annual notices being delivered to consumers in 2002 have been improved relative to the 2001 notices. No doubt we will all learn more in 2002, so that the 2003 annual notices will be better yet. A change in the underlying statutory or regulatory requirements at this early stage will only serve to disrupt the learning process and the valuable dialogue among these constituencies, with the likelihood that confusion will be exacerbated. Similarly, a patchwork quilt of individual state privacy rules and disclosure requirements will lead to greater consumer confusion on this important subject.

8. *The feasibility of different approaches, including opt-out and opt-in approaches, 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?*

Response:
If Bank of America were required to obtain customer consent before sharing information with affiliates, we would, as a practical matter, have to dismantle the customer information management systems we have built to meet our customers' demands. Customers, who generally think of Bank of America as a single enterprise rather than as a collection of affiliated legal entities, would be surprised and frustrated to discover that inaction on their part would cause them the following inconveniences:

- A credit card customer might lose online access to his credit card balance information and transaction history at the bank's website because the bank and credit card systems are no longer able to "speak" to one another.
- ID thieves, who will know that our affiliates will not have ready access to information, will be able to open fraudulent accounts at multiple affiliates and remain undetected for longer periods of time, thus causing great harm individual consumers and greater fraud losses to Bank of America.
- With our centralized databases dismantled to comply with rules prohibiting sharing without customer consent, government requests to information on accounts of suspected terrorists will have to be routed to each affiliate for separate responses, causing delays and inconvenience for law enforcement agencies.
- A securities brokerage customer's deposits are subject to holds because the bank can no longer see that the customer's total relationship with the company.

- A credit card customer incurs late payment charges on his credit card account because the teller at the banking center did not have access to his credit card account information and could not immediately credit his credit card account.
- A checking account customer will be assessed an insufficient funds fee because the bank did not have access to information about the overdraft protection tied to the customer's credit card.
- The bank's collections agent, who will be unaware that the customer has filed a claim for credit insurance benefits, will contact an automobile loan customer about a past due payment.
- Unaware that the customer has told our investment brokerage affiliate that he does not like to receive telephone calls from us, the customer's banker will call him to inquire about his interest in a special home equity loan offer.

These are just a few examples of the many ways that customers will be surprised, annoyed, inconvenienced and even harmed by a rule that effectively prohibits the management of customer information across our enterprise. A consent or "opt-in" requirement would result in significant inconvenience and harm to the majority of our customers. In contrast, the opt out rule imposed by FCRA provides a meaningful way for the small minority of customers who are very privacy-sensitive to exercise control over "non-experience" information without setting the default rule to deny benefits to the great majority of our customers. There are those who would suggest that financial institution affiliates be permitted to share customer information for purposes of servicing accounts and for fraud detection but require customers to opt in (or permit them to opt out) for marketing purposes. The dilemma this poses is that it is not always easy to draw the line between "service" and "marketing". The following are examples of good customer service that could be construed as "marketing":

- A banker calls her customer to alert the customer that a check has been presented for payment against the customer's checking account, but there are insufficient funds in the checking account to pay the presented check. The banker observes that the customer has a Bank of America credit card account and explains that the customer may want to consider overdraft protection tied to his credit card in order to avoid returned check fees in the future.
- A banker notices that his customer has recently obtained a mortgage loan from an affiliate. The mortgage loan balance would qualify the customer for a package of services that include a checking account with no monthly fee and no check printing charges. The customer currently pays a monthly maintenance fee on his checking account and pays for check printing charges. The banker contacts the customer to let him know that he qualifies for the package of services and that converting his checking account will save him over $100 per year in fees, as well as qualify him to receive other services at no additional cost.
- A customer notifies the bank that his loan payment will be a few days late because he has been out of town. The customer explains that he has a new job that requires extensive travel. His banker provides information about direct deposit, online bill payment and automatic payment services that will help him to pay his automotive loan, mortgage, credit card and other accounts even when he

is on the road. At the customer request, the banker is able to set up these services for the customer, schedule automatic payments to the customer's credit card and other accounts with bank affiliates and automatic transfers from the customer's checking to his IRA at the bank's securities brokerage affiliate.

In each of the above examples, the banker was simply doing a good job of helping his or her customer find solutions to their financial needs – solutions that would bring the customer greater convenience, peace of mind and cost savings. In each case, the banker's access to information about the customer's relationships with affiliates enabled the banker to help the customer. And in each case, the banker's activities could be characterized as both customer service and marketing.

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

Response:
As explained above, Bank of America does offer its customers some choices with regard to the uses of information. We afford our customers the choice not to receive marketing offers from us by direct mail, telephone and/or e-mail. In addition, as required by the FCRA, customers may choose to restrict the information shared among our affiliates.

In order to honor customers' direct marketing preferences, we ensure that all outbound direct marketing solicitations are "scrubbed" against a central database of customers who opt out of direct marketing. We have been very careful to explain to our customers that, even when they have opted out of receiving direct marketing, they may continue to receive marketing information inserted with their account statements and when they visit us online or at an ATM, and they may still be contacted by a relationship manager or assigned account representative.

Additional restrictions on the uses of information would be very difficult to manage and would require that we severely restrict the access to customer information we provide to our customer service and banking center staff. Bank of America serves 116 customers every second of every business day. It is not reasonable to expect our customer service representatives and consumer bankers to determine in connection with each of those 116 customer contacts per second whether the service they are providing to the customer is or is not within the scope of the uses permitted by the customer. The only practical way to manage additional limitations on the use of information would be simply to make the information unavailable on any customer. This would require us to dismantle systems that have been developed and deployed over the last decade. Though it is difficult, in the abstract, to estimate the cost of such an effort, it would be quite substantial. Thus, additional limitations would result in both additional costs for our customers and degradation in the service they receive. Moreover, such an effort would defeat much of the systems improvements we have built to make our services more convenient and to provide greater benefits to our customers, and it would negate much of the synergies and benefits that we and other financial institutions expect to derive from the financial

modernization provisions of GLB Act. Such restrictions would also impose significantly greater costs and burdens on financial institutions than those to which other industries are subject, thus putting financial institutions at a severe competitive disadvantage relative to other information-driven industries.