Joseph R. Crouse
Senior Executive Vice President
Legislative Counsel

43

MBNA America Bank, N.A.
Wilmington, Delaware 19884-0127

(302) 432-0716

May 1, 2002

VIA E-Mail: study.comments@ots.treas.gov
VIA Fax: 202-906-6518
Regulations and Legislation Division
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

Gentlemen:

MBNA America Bank, N.A. ("MBNA America") is a national banking association specializing in the marketing of affinity credit cards. Through our agreements with more than 5,000 organizations, MBNA issues credit cards endorsed by colleges and universities, professional sports teams, cause-related organizations, professional trade associations and similar organizations. Additionally, through joint marketing agreements, we issue and service credit cards on behalf of more than 150 banks and credit unions. We are the world's largest independent issuer of MasterCard and Visa credit cards. MBNA America also offers sales finance loans for a variety of retailers, manufacturers and service providers and individual lines of credit for personal, family or household purposes.

Through our affiliate MBNA America (Delaware), N.A. ("MBNA Delaware"), we offer business lines of credit, credit cards for business use and home mortgages. Additional affiliates include MBNA Marketing Systems, Inc. ("MSI") specializing in telemarketing and MBNA Technology, Inc. ("MTI") specializing in information systems, data management and statement production. Formation and organization of all these affiliates (collectively referred to as "MBNA") resulted from various financial, regulatory, fiscal and operational drivers.

MBNA's primary marketing channels include direct mail, telemarketing, direct promotions, and the Internet. MBNA contracts with a wide-variety of nonaffiliated third parties to provide services on our behalf (such as check printing, data processing, telemarketing, direct mail

marketing) and to offer products and services to our Customers outside of MBNA's business lines.

MBNA appreciates this opportunity to comment to the Treasury Department, the federal functional regulatory agencies and the Federal Trade Commission, regarding 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 ("GLBA"). In accordance with the Treasury Department's instructions our responses are identified with the number and letter of the question to which they relate. For convenience and clarity, the Treasury's questions are restated in italics, with our response immediately following. Consistent with the Treasury's questions, the terms "information" and "confidential customer information" mean "nonpublic personal information" as defined in the regulations implementing the financial privacy provisions of Title V of GLBA. In addition, the term "customer" means any individual and includes any individual who applies for or obtains a financial product or service.

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?

For the typical retail credit card customer, MBNA maintains approximately 200 data elements including: (i) identification information (such as name, address, telephone number, e-mail address, Social Security number, date of birth, mother's maiden name or password, and account number); (ii) transaction and experience information (such as purchases, payments, balances, billing disputes and customer service history); (iii) credit eligibility information (such as credit reports); and (iv) other information (such as proprietary scores, group affiliations, privacy preferences and marketing preferences).

All of this information is maintained by MTI for MBNA America and MBNA Delaware. MTI markets no financial products or services. MTI functions exclusively as an agent of MBNA America and MBNA Delaware, providing information systems, data management and statement production services. To the extent such an arrangement can fairly be described as "information sharing", then sharing is total between MTI and each of MBNA America and MBNA Delaware. It is necessary to effect, administer and enforce the financial products and services requested by the customer.

Similarly, MSI offers no financial products or services of its own. MSI functions exclusively as an agent of MBNA America and MBNA Delaware, providing telemarketing services. MSI representatives contacting an interested applicant take the entire application for a financial product over the telephone, request customer consent to obtain a consumer report and load the completed application with all information required for a decision into information systems maintained by MTI for the benefit of MBNA America and MBNA Delaware. Again, to the extent such an arrangement can fairly be described as "information sharing", then sharing is total between MSI and each of MBNA America and MBNA Delaware. It is necessary to effect, administer and enforce the financial products and services requested by the customer.

Finally, information sharing between MBNA America and MBNA Delaware is much more limited. Subject to the Fair Credit Reporting Act's ("FCRA") limitations on the sharing of credit eligibility information between affiliates, MBNA America may share information about retail credit card customers with MBNA Delaware. Such sharing provides MBNA Delaware with a valuable source of leads for mortgage products and allows MBNA America to offer a financial product that may be more appropriate for some customers. The information shared typically includes identification, transaction and experience, credit eligibility (where permitted) and other information as needed to offer a mortgage product efficiently.

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

In many ways, information sharing by MBNA with nonaffiliated third parties is not significantly different from information sharing by MBNA with affiliates. In addition to the services provided by MTI and MSI described above, MBNA America and MBNA Delaware contract with a wide variety of nonaffiliated third parties as service providers. These functions include supplemental telemarketing, information systems, data management and statement production services. Further, these services include capacity capabilities unobtainable within MBNA for items such as direct mail and e-mail.

Similarly, like the information sharing between MBNA America and MBNA Delaware, both these organizations contract with nonaffiliated third parties to offer a variety of financial products and services. Types of information shared here are limited to what is necessary to offer and service a product efficiently. Some information sharing may be limited to identification information. A good example is an endorsing organization's request for a customer list. Other information sharing may involve nearly all aspects of information held by MBNA concerning a customer. MBNA's joint marketing agreements with other financial institutions are good examples. In many cases these nonaffiliated third parties wish to service the customer through their branch network and Internet website systems, keeping MBNA as "transparent" as possible. With product features like overdraft protection (credit card cash advance covering checks written on insufficient funds) and online statements, considerable amounts of information must be shared in a secure environment to service the Customer immediately and seamlessly.

Finally, MBNA America from time-to-time contracts with nonaffiliated third parties to offer a variety of non-financial products and services. We believe our customers may find these offers to be of value and the decision regarding whether or not to purchase is theirs alone. Again, the types of information shared here are limited to what is necessary to offer and service a product efficiently. Typically, information sharing for these relationships is limited to identification information. GLBA prohibits any sharing of "live" account numbers for such purposes and requires that MBNA both disclose its privacy notice and suppress information regarding any customers that opt out. The FCRA prevents our sharing of any credit eligibility information although exceptions exist for our "transaction and experience" information.

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.

Please see our answers to 1(a) and 1(b) above. With the exception of obvious limitations imposed by the FCRA, we see little difference in the types of information shared by MBNA based upon whether the recipient is an affiliate or a nonaffiliated third party. The significant factor is the product or service provided by the affiliate or nonaffiliated third party. MBNA's practice has always been to limit the amount of information shared to what is required to offer a product or service efficiently, to require confidentiality of the recipient, and to limit use of the information shared to the purposes for which it is shared. These basic information-sharing responsibilities were in place long before GLBA required them.

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

Please see our answers to 1(a) and 1(b) above.

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

Please see our answers to 1(a) and 1(b) above.

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

Please see our answers to 1(c) above.

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

Operational limitations, broadly categorized, fall into either practice/contractual or technological categories. Practice/contractual limitations include self-imposed limitations practiced by MBNA because we believe it's the right thing to do and/or those accepted as part of a contract relationship. For example, while we are technologically capable of doing so, we would not search the transactions and experiences of our customers to identify medical or healthcare payments for purposes of assisting a joint marketing agreement party such as a life insurance company avoid potential risks. We know that's inappropriate as good business people. We do not oppose a law or regulation prohibiting something clearly inappropriate. However, we see no evidence that such practices are actually occurring and we are deeply concerned about overly broad laws or regulations that all too frequently cause adverse unintended consequences and stifle legitimate creative efforts.

Technological limitations usually arise from incompatible information, communication, transmission, or information security systems. We typically find that all such issues can be overcome. The challenge is to make the correct cost-effective decision. And in an increasingly competitive environment where resource allocation must be carefully reviewed, there are times when the correct cost-effective decision is not to transact.

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?

Competition between financial institutions, together with the need to preserve customer trust and brand reputation, always work to limit the amount of information shared between financial institutions. In contrast, the instant access and connectivity of the Internet combined with the increasing specialization of financial institutions increases the demand for information sharing in today's marketplace. Federal financial regulatory agencies play a direct role in this process. For instance, the OCC's emphasis on fee income combined with its expansive interpretations of the finder's fee possibilities under the Bank Powers Act, unfortunately led many financial institutions into retail relationships with nonaffiliated third parties for telemarketing of non-financial membership-based products and services which raised privacy concerns beginning in 1999.

MBNA agrees that there must be a balance between information sharing and customer privacy. We believe that GLBA sets that balance appropriately. The political debate in Congress as the legislation progressed, and the comment period during the regulatory process, resulted in a privacy law of national applicability to all financial institutions implemented without significant disruption in the marketplace and without significant unintended consequences for consumers or businesses. We find only two substantive flaws within GLBA, and two false arguments within the privacy advocacy movement, that currently prevent or inhibit the sharing of information.

First, GLBA should clearly recognize an exception from both notice and opt out for credit cards issued by a financial institution on behalf of endorsing organizations. While the private label, maintaining and servicing, and consent exceptions all arguably apply to such information sharing, an explicit exception is preferred. Most MBNA customers request our credit card because of their affiliation with the endorsing organization. By definition, they expect and accept some information sharing between MBNA and that organization. Even if the exception were limited to name, address, telephone number and Social Security number (for data matching only), it would greatly assist MBNA and its endorsing organizations.

Second, GLBA must set a pre-emptive national standard for privacy of financial information. The Sarbanes amendment, allowing states to be more restrictive, is a grave mistake. Turning national banks toward a state-regulated scheme for the privacy of financial information makes no sense, especially as part of a Federal law eliminating the barriers between banking, insurance, and securities businesses. As each state "goes its own way", financial products and services will become more difficult to obtain, less flexible in terms and conditions, and more costly to consumers. MBNA finds this favoritism for states rights quite odd, particularly given the speed with which Congress is ready to dismiss the very same issue where Internet privacy is concerned (see S. 2201, the "Online Personal Privacy Act").

With respect to the privacy advocacy effort, we must question motives when we learn that proposed information sharing restrictions between affiliates seek to distinguish between so-called "good" and "bad" affiliates. Qualitative judgments do not belong here - if a financial institution affiliate is engaged in inappropriate activity such as predatory lending, then predatory lending is

the issue (or facilitating identity theft or illegal telemarketing) to address. Wrapping legitimate issues under the politically popular cloak of "privacy" may get legislation passed and achieve short-term goals, but it won't address the real issues. And that helps neither consumers nor financial institutions.

Finally, the privacy advocacy movement must engage in some cooperative undertakings with the financial industry and provide real data for some of its assertions. Despite all the furor over so-called "privacy incidents" at financial institutions such as U.S. Bank and others, we have yet to see any evidence that sharing of information by financial institutions, either between affiliates or with nonaffiliated third parties, substantially contributes to identity theft or causes any other significant harm. At its worst, it may result in the offer of a product or service that a consumer may not want. The recent dismissal in New York of the privacy class action brought against Chase is a good example. In Smith v. Chase Manhattan Bank USA, (Brooklyn Supreme Court No. 9531B, Justice Nicholas A. Clemente; Dismissal affirmed by 2nd Department), the court found no harm. "Class members were merely offered products and services which they were free to decline. This does not qualify as actual harm".

This is not to say there are not real issues of concern. Correcting credit-reporting inaccuracies, verifying address variations between an application for credit and a credit report, and honoring consumer preferences for information sharing and marketing communications are all worthy topics. The financial industry is ready, willing, and able to not only discuss them, but to take concrete, verifiable steps to address them once a common understanding of the problems and an accepted framework to resolve them are developed.

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.

MBNA employs administrative, technical, and physical protections to safeguard customer information. We do this because it's necessary to protect our business, our customers, and our reputation. We found no specific changes to our practices and procedures required to conform to GLBA's Guidelines for Safeguarding Customer Information because we were doing the things they required long before GLBA became law.

Administrative protections include a variety of policies, procedures, and standards implemented to achieve reasonable levels of security. Examples include our requirements for the length and content of passwords; standards for how often passwords must be changed; verification standards and authorization protocols in our password administration areas; and dual signature or access requirements for particularly sensitive matters or areas.

Technical protections include information security architecture implemented to achieve reasonable levels of security. Examples include careful selection of software and hardware for purchase; constant monitoring of internal and external activity to identify unauthorized access; penetration and vulnerability testing; daily scanning for published vulnerabilities such as viruses,

back doors, and bugs; incident identification, escalation, evaluation, and resolution procedures; file construction, encryption, and transmission protocols including data integrity verification; and a host of other attributes.

Physical security includes the construction, maintenance and operation of our facilities; employee background checks; identification badges and their use; requirements for escorting visitors; nightly "clear desk" policies; document shredding procedures; and restricted entry to particularly sensitive areas.

MBNA evaluates all of these aspects for information sensitive third party service providers. If conditions are found that do not satisfy our standards, we require the vendor to meet them or we go elsewhere. While we are rigid in assuring that our standards for security are satisfied, we are flexible in the means by which reasonable levels of security may be achieved. For instance, if the cost of a vendor upgrading their encryption standards to transmit an electronic file to us on a one-time basis outweighs the cost of securely transporting a magnetic tape of the same information, we may choose the latter method. Balancing costs and benefits to achieve the reasonable level of security is the key challenge in this area.

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)?

We believe, given the size and complexity of MBNA's business, that all of the measures described in 2(a) above are required. Again, we emphasize that we were engaged in all these activities before passage of GLBA and the Guidelines. We believe the standards are reasonable and properly focused on the goal of safeguarding customer information, rather than dictating a particular means or technology to achieve it. Further, the standards recognize that security threats change constantly and emphasize continuous testing, evaluation, reporting, and revision to maintain protection levels.

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

Yes. Please see our answer to 2(b) above.

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

Security is a moving target with constantly evolving challenges. GLBA and the Guidelines provide a useful framework of basic conceptual requirements without driving financial institutions toward particular solutions that may be ineffective tomorrow. Combined with the constant pressure of a competitive financial marketplace, we do not believe any additional requirements in law or regulation would be useful. We also do not support the all too prevalent concept of fines, penalties or private causes of action being added to these regulations. Some security breaches occur which result in no actual harm to consumers. In such situations, piling on the penalties serves neither the marketplace nor consumers in the long run. MBNA does, however, strongly support uniform standards for data transmission and encryption by and among

government agencies. The Federal government is uniquely positioned to lead the way in areas where individual businesses may fear to tread due to lack of accepted standards.

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?

Information sharing with an affiliate possesses no unique potential privacy risks to customers. MBNA's affiliates are part of the same corporate structure - all our affiliates are subject to the same control mechanisms for ensuring information security and confidentiality. Admittedly, any time information is shared there is a risk of unauthorized access or failure to maintain confidentiality. However, we know of no such situations arising from information sharing among affiliates and emphasize that in this situation, the same financial institution controls both ends of the transmission.

MBNA acknowledges that a financial institution may have business operations organized within affiliates in such a way that aspects of information sharing may be inappropriate. As mentioned earlier, we would not support a credit card operation providing a life insurance affiliate or joint marketing agreement party with information regarding payments made by customers to healthcare providers for purposes of avoiding risks. Similarly, we would not support a health insurance affiliate providing information about seriously ill customers to a mortgage affiliate for purposes of preventing mortgage offers to such customers or accelerating existing mortgages. Again, we have seen no evidence of financial institutions doing such things.

While harm to consumers is possible if information sharing occurs among affiliates for impermissible purposes, MBNA believes information sharing among affiliates generally benefits consumers in two significant ways. First, we believe that sharing of information among affiliates reduces potential risks to customers by helping prevent fraud and identity theft. The more relationships a financial institution has with a customer, the better able they are to anticipate their needs. This includes not only the ability to offer them products and services they may be interested in, but also to detect inquiries, transactions, or events that may be out of the ordinary. The fraud detection schemes employed in the credit card industry to detect unusual activity are a prime example of how information sharing benefits and protects customers. The more inputs there are to that system, the more accurate its predictions and the more transactions of a given consumer it may protect.

Second, consumers benefit from additional product and service offerings in a number of ways. Strictly from a marketing perspective, identification information sharing between affiliates keeps costs down – the same prospect data does not need to be acquired and paid for twice. Even if one consumer does not desire the offered product or service, this sharing keeps the costs down for those that do. Further, many institutions offer reduced rates, fees or other charges for additional products or services when a customer obtains a second product or service. Affiliate information sharing increases these possibilities – the "relationship pricing" offered by many credit unions is a good example of this practice. To maintain these programs, these institutions

need information about all their relationships with a customer across all affiliates (and sometimes with nonaffiliated third parties or joint marketing agreement parties).

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?

In the abstract, it's easy to believe that potential privacy risks increase when a financial institution shares information with a nonaffiliated third party. Indeed, unlike information sharing between affiliates, the sharing financial institution only controls the transmitting end of this relationship. However, a rational assessment quickly reveals the false prejudices underlying this abstract assessment.

First of all MBNA credit cards are handed over millions of times a day by our customers to total strangers. This is how we pay for goods and services and the volume of these transactions and their financial value increase every year for one simple reason – it's safe, accurate and convenient. Yes – fraud and identity theft may occur –in fact they are better documented at this stage of the payment process than at any other stage of information sharing by financial institutions. Unfortunately there will always be dishonest employees at retail businesses who improperly obtain or retain payment information and use it inappropriately. MBNA supports laws that criminalize identity theft and we urge Federal, state and local law enforcement agencies to enforce these laws, prosecute the criminals and impose the penalties. We didn't stop using banks or cash when criminals started robbing banks and we should not stop using payment devices and sharing the information needed to support them when criminals start to abuse them. It's the improper use of information that's at issue - not information sharing.

Second, while MBNA provides many of its services directly through MBNA affiliates to its customers, like our competitors we also use nonaffiliated third party service providers. Indeed, many issuers outsource the entire statementing and customer information system (CIS) to such vendors. We are not aware of a single instance where a financial institution using the services of an information processing or statementing vendor compromised the privacy of its customers. And that's no accident. Such relationships depend on the quality of the services provided. Nonaffiliated third parties receiving information from financial institutions have been bound for years under contracts to maintain confidentiality and to use the information only for authorized purposes. Any vendor that fails to do this loses its customers – and won't get any new ones.

GLBA and the Guidelines ensure strict security and confidentiality. They require appropriate due diligence of a nonaffiliated third party's information handling practices, written agreements to not use or disclose the information other than for a specified purpose, establishment of an adequate information security program, and maintenance of the program while the third party possesses the data. Further, all of these requirements fit well with the powers of the Federal functional regulators under the Bank Service Company Act, 15 USC §45(a)(2). GLBA consciously avoided making financial institutions behave as one another's policeman, and MBNA is concerned about proposed State legislation that appears to go beyond GLBA's requirements in this regard (California AB 1775).

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?

All affiliates of a financial institution are subject to the internal controls of that organization with regard to information usage. We do not believe that interaffiliate sharing of information with a nonaffiliated third party poses any different privacy risk than those associated with the direct sharing of information by the financial institution with a nonaffiliated third party.

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?

Please see our answer to 3(a) above. The benefits to financial institutions include additional and deeper customer relationships, superior fraud detection, and the ability to offer packaged services and benefits.

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

Please see our answer to 3(b) above. The benefits to financial institutions include additional and deeper customer relationships, superior fraud detection, and the ability to offer packaged services and benefits. Additionally, services provided by nonaffiliated third parties are frequently higher in quality and lower in cost than those a financial institution could provide for its customers. Lastly, with respect to joint marketing agreements between two or more financial institutions, information sharing allows immediate service of the customer at any point of contact and a seamless interface from the customer's perspective.

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

Please see our answer to 4(a) above.

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

Please see our answer to 3(c) above. We point out that with an affiliate specializing in information systems and data management, information shared by one affiliate to another affiliate for business purposes will be shared with the information systems and data management affiliate routinely.

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

MBNA believes further privacy restrictions are unnecessary, will inhibit the business flexibility and creativity of financial institutions, will create unintended consequences - hampering customer convenience and the ability to control fraud and administer the customer relationship

beyond an "account-by-account" basis. Further, to the extent privacy is being used as a vehicle to reduce marketing contacts or address identity theft concerns, MBNA believes those issues should be addressed directly.

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?

Please see our answer to 4(a) above.

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

Please see our answer to 4(b) above. The benefits to customers include more and better financial products and services from which to choose, superior fraud detection, real time instantaneous access to all of the customer's financial information, and the ability to obtain packaged services and benefits.

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

On a broad scale, MBNA agrees with the findings of the Financial Services Roundtable set forth in their December 2000 report entitled, "Customer Benefits from Current Information Sharing by Financial Service Companies". There is no question that information sharing increases the availability of credit to the market in general and reduces the cost of credit to the customer. For MBNA in particular, the ability to make consumer credit decisions in minutes has been and will continue to be an important marketing advantage.

Customers of financial institutions obtain significant benefits from information sharing, including increased convenience, personalized service, 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 study estimated the benefits to customers of the 90 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' customer, on average, $195 per customer household per year. In addition, the average household saves close to 4 hours per year due to the convenience provided by information sharing.

- Money Saved. For all customers of the Roundtable's members, the current dollar savings due to information sharing total about $17 billion per year. About $9 billion of this total comes from information sharing with nonaffiliated third parties, and about $8 billion is

due to 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 nonaffiliated third parties.

- Sources of Benefits. Customers benefit from information sharing across a wide variety of services. They save money from outsourcing to nonaffiliated third parties, relationship pricing, and proactive offers. Customers save time because of information sharing by call centers, Internet based services, nonaffiliated 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 the Roundtable survey include:

- A large share of time and money saved is from nonaffiliated third party services, a subset of all benefits from sharing with nonaffiliated third parties. Many financial institutions are seeking to provide "one-stop shopping" through a full range of financial services, and are partnering with nonaffiliated third parties to provide their customers with low-cost, efficient services (e.g., credit cards, insurance). Using nonaffiliated 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 and $7 billion annually.

- Call centers provide significant savings of time. Companies integrate their call centers for different affiliates and/or nonaffiliated 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 nonaffiliated third parties, saving customers over $2 billion a year.

These information-sharing benefits only account for the savings provided by the 90 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.

These estimates do not include:

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

MBNA 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. Information sharing is a critical component of our business, and if financial institutions do not share among themselves the only likely alternative is a centralized information sharing organization. We do not believe our customers would look favourably on such a concept, whether operated collectively by financial institutions or the government.

e. What effects, positive or negative, would further limitations on the sharing of such information have on 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 nonaffiliated third parties, these benefits to customers – up to $17 billion of cost savings and 320 million hours of timesavings 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 institutions.

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.

MBNA believes that FCRA and GLBA provide adequate protections for customer privacy. Further, Federal law includes numerous additional privacy protections, such as the Electronic

Fund Transfer Act and the Right to Financial Privacy Act. Affiliate sharing of credit eligibility information has been dealt with through opt out under the FCRA for years. GLBA follows the same concept, requiring a clear and conspicuous notice from each financial institution to each customer setting forth their opt out rights under FCRA and GLBA and providing a convenient means for customers to effect those opt outs.

Opt out provides the appropriate balance between protecting customer privacy and permitting the sharing of information by financial institutions. It allows most information sharing to continue by financial institutions as it has for many years. Simultaneously, it allows those customers particularly concerned about the sharing of financial information to exercise their rights and opt out. An opt out standard is incorporated in numerous Federal laws and courts do not favour more restrictive regimes, such as outright bans or opt in regimes (U.S. West, Inc. v. Federal Communications Commission, U.S. Ct. App. 10th Cir., No. 98-9518, filed August 18, 1999).

The only problem with existing law is GLBA's failure to establish a national uniform standard for the privacy of financial information. By permitting individual states to enact different customer protections, GLBA opens the door to confused customers and unbelievably complex and expensive compliance responsibilities for financial institutions. A patchwork of state laws with differing requirements and different levels of protections will diminish the benefits to customers described above, increase confusion of customers' understanding of their rights, add to the compliance responsibilities of financial institutions, and add to the costs of providing products and services to customers.

GLBA is less than one year old. Experience to date has not produced any evidence of 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.

MBNA believes that a uniform national standard should be made a permanent part of GLBA, as it was for seven years under the FCRA. We recognize that such uniformity is set to expire under the FCRA, but we 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 FCRA and should be embraced for GLBA. Otherwise, the real benefits of a uniform national information-sharing regimen will be significantly diminished.

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.

MBNA believes that financial institutional privacy notices have been adequate under the existing law, but they have also been overly complex and legalistic. The disclosure requirements of

GLBA were new to consumers, financial institutions, and their regulators in 2001 and they took effect at a time when the class action plaintiff's bar and the State Attorneys General had both focused on privacy of financial information. To meet these new requirements, financial institutions worked very hard – establishing working groups internally, retaining legal counsel, using consumer focus groups externally, and following the sample language provided by the Federal functional regulators. The disclosures were necessarily detailed because of the complex statutory and regulatory requirements and fear of litigation and potential liability compounded the problem. The process resulted in perhaps more thoroughness than meaningfulness.

MBNA's initial privacy notice complied with all GLBA and FCRA requirements and was developed mostly from sample language in the GLBA regulations. Even so, advocacy groups judged our notice, like those of almost all other financial institutions, as hard to read and understand. For MBNA's first annual privacy notice disclosure in 2002 we are working hard to address those concerns.

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.

Privacy notices must be standardized. Like the nutrition labels placed on foods, they must appear in an easily recognized form, become shorter, and become easier to understand. A uniform, user-friendly privacy notice will increase the level of trust between financial institutions and their customers.

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.

While MBNA has seen no definitive studies, we agree that opt in percentages will parallel opt out percentages. This means that an effort to obtain opt in from a financial institution's customer base will yield only 2% - 5%. Quite frankly, that is not a sufficient return to authorize significant investment in the systems required to track the issuance of opt in notices and record the receipt of opt in responses. From an economic standpoint, financial institutions will simply forego pursuing the opt in; a phenomenon already demonstrated under Vermont's financial privacy regulations which took effect February 15, 2002.

Consequently, all information sharing restricted to opt in privacy protection would cease and all customer benefits flowing from such information sharing would terminate. While exceptions under such regulations would most likely provide for continued information sharing to service and process transactions requested by the customer, to accrue points or rewards, and to respond

to legal requirements, we question the need for such a disruptive standard. What is the need for the change; what is the governmental interest being served? If the issue is identity theft or annoying marketing contacts – let's deal with them directly. If the issue is customer's who don't want a financial institution data mining their transaction history to predict what financial service or product they might be responsive to, then why doesn't opt out work?

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.)

Law and regulation are not the place for voluntary scenarios. If the issue is important enough to require a law or regulation, then it is important enough to set a definitive, mandatory, and uniform national standard. Any further "fractionalisation" of the financial privacy issue will marginalize the outcome for everyone.

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

MBNA spent millions of dollars to build its privacy notice disclosure tracking and opt out recording system. We spent millions more developing, printing and mailing our privacy notice and we will continue to do so every year hereafter. We are proud of our efforts and certain that we have satisfied both GLBA and FCRA requirements. The fact that we have a working opt out system to screen information sharing with nonaffiliated third parties and credit eligibility information sharing with affiliates proves we could construct an opt out system for information sharing with affiliates generally.

Current estimates are that only 2%-5% of all customers opt out of information sharing with nonaffiliated third parties under GLBA. This means either that the overwhelming majority of consumers are quite satisfied with the status quo, that they don't care about the financial privacy issue as much as the privacy advocates would like you to believe, or that they do not read what's sent to them in the mail regarding their financial products and services. Whatever the truth may be, there is no clear driver for increasing restrictions. This is especially true where the consequences of increased restrictions on affiliate information sharing are unknown. Information may have to be provided to affiliates so that the disclosing institution can provide services to customers, or receive services necessary to operate its business. For example, MBNA America obtains information systems, data management and statement services from MTS and obtains telemarketing services from MSI. Access to customer information may be required to perform all these functions in the ordinary course of business.

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.

Other than opt out or opt in, we are not aware of any other method that permits customers to direct that information not be shared with affiliates or nonaffiliated third parties. But we are not sure that "privacy" is best protected by laws and regulations focusing on information sharing to begin with. The rest of the world, including the European Union, Canada and most Asian and Pacific nations, follow a system of data protection focused on fair information practices rather than information sharing. While we have reservations about the centralized data protection bureaucracies these types of laws tend to create, we cannot deny that they seem to be working for the countries which adopt them and may be, overall, less disruptive to our industry than GLBA, FCRA and multiple state-level variations may be.

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?

MBNA does not share information for inappropriate purposes and while we see no evidence that additional laws or regulations are necessary to prevent such activity, we do not oppose them. We do oppose further restrictions on information sharing that are really attempts to deal with other issues, such as marketing methods or "predatory" lending. Similarly, while not opposed in principle to limitations on so-called "sensitive information" (sexual orientation, religion, political affiliation), we see no evidence that financial institutions are sharing such information and therefore question the need for such laws and regulations. Finally, we fear that further restrictions on information sharing will stifle creativity and prevent financial institutions from keeping pace with other sectors of the economy as data connectivity and the ability to predict customer behaviour improve over time. Disadvantaging the financial services industry in such matters makes no sense. Restricting the sharing of information for specific uses or directing the specific uses for which the information may be shared are generally unworkable if customers are to continue the benefits they currently enjoy.

MBNA respects and understands the importance of customer choice. We built our business of issuing credit cards for endorsing organizations upon choice. But we believe in choice for a purpose. Our business depends on information and we cannot operate in an environment requiring individualized information sharing for each customer, or each state in which they reside. Our business is providing top-quality financial products and services – not privacy systems. We are ready, willing and able to incorporate into our operations carefully considered privacy limitations applying to all commerce nationwide. We are not prepared to accept, and we will oppose, laws and regulations needlessly imposing exorbitant costs and mind-boggling complexity upon our industry, with no more evidence that they are necessary than the self-proclaimed right to privacy and political expediency.

Neither Congress nor the Federal functional regulators will have to answer the dissatisfied customer who cannot understand why they must provide all of their personal information to MBNA Delaware to obtain a mortgage when considerable portions of that information are

already on file with MBNA America for their credit card. MBNA will answer that dissatisfied customer, and we will tell them exactly what happened and who brought it about.

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

MBNA accepts that customers want privacy choices and we believe they want those choices presented in a standardized, easy to understand format. We believe GLBA establishes appropriate and manageable choices and that financial institutions are rapidly simplifying how customers may exercise them. Further restrictions on information sharing and further requirements that customers be able to direct aspects of sharing for particular items of information will be more confusing to consumers, more costly to administer, more likely to increase fraud and identity theft, and will increase the costs of financial products and services.

If you have any questions, please contact me at MBNA America Bank, N.A., 1100 North King Street, Wilmington, Delaware, 19884-0127. My phone number is 302-432-0716. My facsimile number is 302-432-0753 and my e-mail address is joseph.crouse@mbna.com.

Sincerely,

Joseph R. Crouse
Legislative Counsel