AMERICAN BANKERS ASSOCIATION ®

1120 Connecticut Avenue, NW
Washington, DC 20036

1-800-BANKERS
www.aba.com

25

World-Class Solutions, Leadership & Advocacy Since 1875

James D. McLaughlin
Director
Regulatory & Trust Affairs
Phone: 202-663-5324
Fax: 202-828-4548
jmclaugh@aba.com

April 30, 2002

Regulations and Legislation Division
Chief Counsel's Office
Office of Thrift Supervision
1700 G Street, N.W.
Washington, DC 20552

Attn: Study on Gramm-Leach-Bliley Act Information Sharing

Dear Sir and Madam:

The American Bankers Association ("ABA") is pleased to respond to the Department of the Treasury's request for comment regarding its study of information sharing practices among financial institutions. The ABA brings together all categories of banking institutions to best represent the interests of this rapidly changing industry. Its membership - which includes community, regional and money center banks and holding companies, as well as savings associations, trust companies and savings banks - makes ABA the largest banking trade association in the country.

In our response, we have provided a review of the practices generally found within the financial services industry. These information sharing practices will vary, to some degree, across financial institutions, depending upon the institution's size and scope of financial services.

The privacy provisions contained in the Gramm-Leach-Bliley Act, in conjunction with numerous other federal privacy laws already in place, represent a rigorous, comprehensive and carefully constructed scheme of federal privacy protections for financial institution consumers. These laws subject financial institutions to an extensive regime of privacy regulations, and should be given time to work before any modifications at the federal level are envisioned. Similarly, efforts by the states to change existing laws or adopt new laws that impose additional layers of privacy regulation are likely to, at best, complicate implementation of Gramm-Leach-Bliley. At the very worst, changes can undermine consumer benefits and adversely affect current information practices designed to protect institutions and consumers alike from fraud and other illegal activities that are built into the new federal privacy law.

In addition, it is critical that any study of information practices consider consumer reaction. For example, the ABA filed a Freedom of Information Act (FOIA) request with the four banking agencies to determine the amount of complaints on GLB privacy notices in 2001. The responses are instructive. The Federal Reserve Board received a total of 4503 complaints from all categories. Of those 4503, only 25 related directly to GLB privacy notices or .0056% of all complaints. The Office of Thrift Supervision (OTS) received 4921 total complaints in 2001. No complaint was related to the GLB notices. There were only 6

privacy related complaints or .0012% of the total.[1] Clearly, it can be inferred from these responses, that consumers are generally satisfied with the industry's handling of the new privacy laws and regulations.

Finally, any effort to make distinctions between information sharing among financial institutions and their affiliates and sharing among institutions and third party providers of financial services will severely impact the ability of community-based financial institutions to compete. Such distinctions are artificial, in that the sharing of information in either case is for the same purpose: to provide quality financial services to consumers.

If you have any questions or comments, please contact me at (202) 663-5324.

Sincerely,

James D. McLaughlin

[1] Similarly, the FDIC and the OCC FOIA responses did not specifically cover the GLB notices. Instead the FDIC noted 6849 total complaints and only 137 that were privacy related (.0200%) The OCC received 17228 complaints and 368 or .0214% were privacy related.

ABA/Treasury GLB Survey

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?

Within their family of companies, financial institutions generally share information such as name, address, etc. From time-to-time, institutions will also share information regarding the financial products and services a customer purchased with an affiliate in order to make other appropriate financial products available to that customer.

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

According to a survey of 390 financial institutions on August 20, 2001 conducted by the American Bankers Association[2], 89 percent of these institutions did not share information outside of the exceptions under the Gramm-Leach-Bliley (GLB) Act and Regulation P.

Under the exceptions granted by the GLB Act and Regulation P, institutions commonly share nonpublic information about customers in order to service loans or accounts or to respond to legal requirements. For instance, institutions will report a customer's credit experience to consumer credit reporting agencies as authorized by the Fair Credit Reporting Act.

All sizes of financial institutions, but particularly community banks and other smaller financial institutions, share information such as name and address with third party marketers of financial products. The ability to share this information is vital to community-based institutions; as such institutions have a greater tendency to depend on third-party providers to offer their customers a full range of financial services.

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.

As a general rule, some financial institutions chose to offer customers a full range of financial services through affiliates, while others provide such services through third parties. In both cases, the information needed to offer or complete these financial transactions is essentially the same.

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

To provide additional financial products and services to customers not provided by the financial institution but by an affiliate of the institution.

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

---

[2] "Survey on Privacy Policy Responses," American Bankers Association, August 2001.

To affect transactions initiated and/or authorized by the customer to process account transactions, such as processing check order requests or to provide electronic banking services.

To provide additional financial products and services to customers not provided by the financial institution but by a third party with which the Bank has a joint marketing agreement that contains confidentiality provisions.

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

In limited instances, financial institutions have decided to voluntarily offer customers the chance to opt out of affiliate information sharing. This is and should remain a voluntary management decision on the part of the financial institution.

g) **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?**

Financial institutions remain interested in sharing information on fraud-related activities among other institutions to prevent and detect such crimes. The ability to share such information was supposed to be clarified by the promulgation of a rule implementing Section 314 of the USA Patriot Act. For the reasons discussed in the attached comment letter previously filed by ABA on that proposal, we are urging modification of that process. (See attached)

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.**

Financial institutions utilize a wide variety of security procedures, which limit access to information. Access is generally limited to employees with a "need-to-know" job-related basis. Information is also only given to third-party service providers pursuant to written contracts that contain confidentiality provisions.

Financial institutions are required by the GLB Act (501 b) to have comprehensive Information Security Programs that provide strong protection for customer information:

Information Systems Security Policy and Staff Training: A comprehensive Information Systems Security Policy approved by the Board of Directors and distributed to all business unit managers. Generally an abbreviated version of the policy is distributed to all financial institution employees.

System Risk Assessment: A system risk assessment for all mission critical platforms. These assessments address logical access controls, physical restrictions and controls, encryption, change controls, staff controls, monitoring, ERT response, backup and contingency planning, tests and audits, service providers, and public/non public information resident in the system. The assessment identifies risks, threats, and controls.

Vendor Due Diligence: A vendor due diligence document that guides Business Unit Managers in the selection and management of vendors.

Network Security Vulnerability and Penetration Testing: Network security vulnerability and penetration testing as defined in FDIC FIL 68-99. Testing is performed on a quarterly basis and includes social engineering, modem penetration, Internet penetration, server and physical site assessment.

Managed Security Network Services: Managed security network services on a 24 hour a day, 7 days a week basis including holidays. These services are designed to address Internet and network security concerns for monitoring, prevention, detection and response as defined in FDIC FIL-67-00.

Incident Response Services: Third party incident response services. These services include identification and classification, notification and escalation, containment, eradication, recovery and follow-up, and legal authority liaison.

Disaster Recovery & Business Continuity: Testing of the financial institution's capability of recovering their mission critical platforms at offsite locations as defined in FFIEC SP-5. Platforms tested include the mainframe, networks, core applications, proof and capture processes, personal computer application, file transmissions, application functionality testing from office locations connected to the service provider, and IVR telephone lines switching. The Board of Directors is provided with test results annually.

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)?

While existing law currently mandates all the safeguards described above, many were in place at financial institutions long before the GLB Act and Regulation SP.

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

Yes. The more critical need is for consumers to be properly educated regarding their responsibility to protect themselves from identity theft and fraud and assert their positions regarding telemarketing.

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

None. Just over two years ago, Congress carefully considered the costs and benefits of the privacy-related restrictions that ought to apply to financial institutions and their consumers, which resulted in Title V of the GLB Act. Financial regulators subsequently implemented detailed privacy regulations for the first time, and financial institutions have spent many millions of dollars to build systems to comply. Financial institution customers now enjoy the benefit of those protections, which ought to be given a chance to work.

Privacy compliance is costly, particularly for community banks. According to TowerGroup, large money center banks spent as much as $25 million developing GLB compliance systems, plus the printing and mailing privacy disclosures, in addition to adding and training staff to handle consumer responses. The firm estimates that most

independent and smaller banks spent between $100,000 and $250,000 each to comply with the privacy provisions within the Gramm-Leach-Bliley Act.

Title V of the GLB Act protects customer information in both the online and the offline environment. Any law further restricting online use, such as the proposed Senate Bill 2201, for example, would disproportionately subject financial institutions to a whole new layer of privacy regulations that would apply at the same time as those imposed by the GLB Act and other financial privacy laws. That would mean two types of notices to customers, two types of consent provisions, redundant security requirements, and two distinct types of enforcement regimes. Rather than protect and help customers, these redundant requirements will needlessly confuse and annoy customers. At the same time they would be far too burdensome and costly. Financial institutions should be subject to a single privacy regime that applies equally in all contexts.

Individual state provisions frustrate the efficiencies of the holding company structure by making the treatment of customer information specific to each state. Such provisions impose a greater regulatory burden than individual state laws requiring certain disclosures in a mortgage and other transactions, in that they go to the very heart of how a financial institution handles customer personal financial information on a day-to-day basis, not just as it relates to a specific one-time transaction.

3) The potential risks for customer privacy of such sharing of information:

a) What, if any, potential privacy risks do customers face when a financial institution shares the customer's information with an affiliate?

As with any transaction, there is always the minimal risk that customer information is used in some manner for which it was not intended. Financial institutions and holding companies that actively control this risk through strict compliance with the corporate privacy policy greatly reduce this risk.

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?

As with any transaction, there is always the minimal risk that customer information is used in some manner for which it was not intended. Financial institutions and holding companies that actively control this risk through strict compliance with the corporate privacy policy greatly reduce this risk. Third party agreements also contain specific confidentiality agreements limiting the reuse and redisclosure of customer information provided the third party. In addition, GLB clearly prohibits the reuse of information. Most of these nonaffiliated third parties have no need to retain customer information for performing the outsourced tasks, limiting customer privacy risk.

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?

No greater level of risk than noted in the previous section.

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?**

Among other things, sharing information with affiliates enhances an institution's ability to cross-market an extensive array of financial products, tailored to a customer's specific needs.

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

The greatest benefit is to community banks and other small financial institutions that do not have the infrastructure and resources to provide competitive services without utilizing third party providers of financial services. These institutions benefit greatly by outsourcing processes to nonaffiliated third parties. Customers of those institutions receive these products at competitive prices.

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

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

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

Community banks would be highly disadvantaged if they could not rely on third party service providers for account processing needs and for products managed more cost effectively by specialist third party service providers.

Also, due to the unique bank and financial services holding company structure in the United States, separate corporate affiliates are encouraged. Any limit on information sharing among affiliates would run counter to our existing financial system that, either by regulation, law, tax or organization demands separate entities over consolidation.

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

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

Customers' benefit from financial institution affiliate sharing because they receive information specifically targeted to them. For instance information on college savings plans to families with children, information on home equity products can be sent only to homeowners. Targeted marketing decreases the amount of "junk" mail or solicitations the customer receives, and gives customers the chance to build a relationship with affiliates, thus strengthening their relationship with the bank. Targeted marketing also benefits the bank by saving on production costs and mailing costs.

As detailed in a recent study by Ernst & Young[3] for the Financial Services Roundtable, financial institutions seek increasingly to provide a full range of financial services to their customers, call centers often need to share information with affiliates or third parties to provide customers with the convenience of using a single phone number. Customers with numerous financial products from the same institution expect the ability to access their deposit accounts, investments, insurance policies, credit cards, and mortgage loans with one phone call. They do not want to have to call multiple phone numbers to change an address, check an account balance, or transfer funds. In addition, having a centralized call center with shared information allows companies to better serve their customers through proactive offers and fraud prevention.

Customers with financial products from different affiliates or third parties also benefit from the ability to obtain information or transact business across multiple services at one integrated Web site.

The Ernst & Young study also found that financial service organizations often use customer information to improve the quality of service provided to the customer. Two means of actively seeking to improve service through access to information are relationship pricing and proactive offers.

For instance, many financial institutions provide customers with discounts on services based on existing relationships, wherein customers get a reduced price for purchasing certain bundles of financial services. Customers may also qualify for reduced or waived fees, lower interest rates on loans, and other price reductions, based on existing relationships. The provision of these price reductions often relies on the ability to share information across affiliates or third parties. Without access to this information, financial institutions would not know whether customers had multiple relationships and qualified for price reductions.

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

It would be a mistake for policymakers to differentiate between affiliate and third party information sharing. Customers benefit from the sharing of information with nonaffiliated third parties in much the same way they benefit from affiliate sharing.

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

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

None.

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

See Answer 5a.

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

[3] "Customer Benefits from Information Sharing by Financial Service Companies," Ernst & Young Economics and Quantitative Analysis, September 2000.

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.**

The current legal framework is more than adequate. Under existing law, consumers have a variety of tools to assert their privacy rights. There has also been no outcry from the public for more privacy laws since GLB was enacted. (See the FOIA responses outlined in our cover letter) Over 98 percent of financial institutions responding to the August 2001 ABA survey indicated their institution received few customer inquires relating to the institution's privacy policy. On average, about 4% of customers communicated with their financial institution in some fashion - usually by telephone – regarding their privacy notice.

In the August ABA survey, only 54 percent of consumers felt they were somewhat or very aware of the privacy protections that existing law provided them, yet these protections are numerous:

The Fair Credit Reporting Act (FCRA) contains many important privacy safeguards. It gives consumers the ability to stop the sharing of their credit application information or other personal information (obtained from third-parties, such as credit bureaus) with affiliated companies. The law permits sharing of information with affiliates regarding the consumer's performance on the loan or other "experience" resulting from the relationship between the consumer and the financial institution.

Moreover, it is important to note that the FCRA allows only affiliated companies to share such application or credit bureau information, after provision to the customer of notice and an opportunity to opt-out. If a financial institution were to share such information with an unaffiliated third-party, it could become a consumer-reporting agency subject to burdensome, complex and onerous requirements of the existing FCRA.

The FCRA also mandates that other notices be provided to consumers in connection with the sharing of information. For example, financial institutions are required to notify consumers when adverse action is taken in connection with credit, insurance, or employment based on information obtained from an affiliate. This notice must inform the consumer that he or she also may obtain the information that led to the adverse action simply by requesting it in writing.

The FCRA also gives consumers the power to stop unwanted credit solicitations by blocking the use of their information from pre-screening by consumer reporting agencies. Pre-screening is the process in which a consumer reporting agency prepares a list of consumers who, based on the agency's review of its files, meet certain criteria specified by a creditor who has requested the prescreening. The FCRA also mandates that providers of credit include disclosures with every solicitation explaining that the offer results from a pre-screening and that the consumer has the right to be excluded from future pre-screenings by notifying the consumer reporting agency.
The Electronic Fund Transfer Act and its implementing regulation require that consumers be informed about a financial institution's information-sharing practices with regard to all accounts that may incur electronic fund transfers. This would include virtually all checking, savings and other deposit accounts.

Financial institutions are required to provide consumers with extensive disclosures at the beginning of the consumer's relationship with the institution. As part of these initial disclosures, each financial institution must state the circumstances under which it (in the

ordinary course of business) will disclose information concerning a consumer's deposit account to third parties. For purposes of this requirement, the term "third-parties" also includes other subsidiaries of a financial institution's parent holding company.

The Right to Financial Privacy Act protects consumer records maintained by financial institutions from improper disclosure to federal government officials or agencies. Historically, the most significant privacy concern of consumers relates to *government* access to their financial records. The Act currently prohibits disclosure to the federal government of records held by certain financial institutions unless there is some form of "due process" or without providing notification to the consumer whose records are sought and the expiration of a "waiting period," during which the consumer may challenge and prevent disclosure through legal action.

The Telephone Consumer Protection Act (TCPA) gives consumers the right under federal law to stop telemarketing calls from a particular company.

Under TCPA, companies can make telemarketing calls to residential telephones only if:

- the call occurs between 8 a.m. and 9 p.m. (local time at the called party's location);
- the caller provides certain identifying information to the consumer; and
- the company maintains a company-specific "do-not-call" list of persons who do not wish to receive telephone solicitations made by or on behalf of the company.

If a consumer wishes to opt-out of future telemarketing calls from a particular company, the consumer only need indicate that he or she does not wish to be called again. The company then must add the consumer's name to the company's "do-not-call" list.

In addition, TCPA protects consumers by restricting the use of automatic telephone dialing devices and prerecorded or artificial telephone messages.

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

There is no need for new laws but a clear need for aggressive enforcement of laws designed to punish privacy violators such as the federal identity theft laws. (18 USC 1028).

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.

While last year's financial institution privacy notices were adequate to meet existing legal and regulatory requirements, there may be room for improvement. Given the stringent privacy requirements under GLB, many institutions have found it a challenge to construct privacy notices that are easily readable and still comply with the regulations. Many of our members utilized the "sample language" released by the agencies. It now appears that

policymakers are criticizing those same models. Institutions are currently working hard to increase the readability of the notices.

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.

No new requirements are necessary. There are many existing tools to help consumers understand their privacy rights, and institutions can work within the framework of existing law and regulation to improve notices.

The FDIC and the FTC have consumer friendly resources for guidance in privacy rights and identity theft protection. The FTC's "Sharing Your Personal Information: It's Your Choice" is worthwhile and relatively unbiased consumer advice.

There has been discussion of the development of a "short form" privacy notice, which has some appeal to the extent that institutions are not held liable for an omission on the form and are instead allowed to point customers toward the full privacy notice to the extent more information is desired.

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.

Opt-in would result in operational difficulties and expenses (ultimately passed on to the customer) that would far outweigh benefits to consumers, already protected, assuming they exercise rights under existing law.

Any restriction on affiliate sharing would negatively affect customers and institutions. . Institutions have built data systems under the assumption that information sharing would continue to be permitted. To prohibit affiliate sharing now would require institutions to replace and reprogram systems at significant expense.

As demonstrated by Fred H. Cate[4] and Michael E. Staten[5], in their paper, "The Fallacy of Opt-In:"

> **1. An "opt-in" system does not increase privacy protection.** "Opt-in" and "opt-out" both give consumers the final say about whether his or her information is used. Neither approach gives individuals greater or lesser rights than the other. Under either system, it is the customer alone who makes the

[4] Professor of Law, Harry T. Ice Faculty Fellow, and Director of the Information Law and Commerce Institute, Indiana University School of Law—Bloomington.

[5] Distinguished Professor and Director of the Credit Research Center, The Robert Emmett McDonough School of Business, Georgetown University.

final and binding determination about data use.

2. An "opt-in" system is always more expensive than an "opt-out" system. An "opt-out" system sets the default rule to "free information flow" and lets privacy-sensitive consumers remove their information from the pipeline. In contrast, an "opt-in" system sets the default rule to "no information flow," thereby denying to the economy the very lifeblood on which it depends. Companies that seek to use personal information to enter new markets, target their marketing efforts, and improve customer service must rebuild the pipeline by contacting one customer at a time to gain their permission to use information. "Opt-in" is more costly because it fails to harness the efficiency of having customers reveal their own preferences as opposed to having to explicitly ask them.

3. Opportunities are lost under "Opt-In." By adopting a default rule that stops the free flow of information, "opt-in" impedes economic growth by raising the costs of providing services and consequently decreasing the range of products and services available to consumers. "Opt-in" would deny opportunities to consumers who now receive unsolicited material by phone or mail and have the option to act on those solicitations. "Opt-in" systems impose extra costs on everyone, *regardless of privacy sensitivity*, as compared to "opt-out" systems.

4. "Opt-In" reduces competition and raises prices. Switching from an "opt-out" system to an "opt-in" system would make it more difficult for new and often more innovative, firms and organizations to enter markets and compete. It would also make it more difficult for companies to authenticate customers and verify account balances, and thus frustrate the ability to counteract fraud. For both reasons, prices for many products would likely rise.

5. A move toward "opt-in" systems is contrary to consumer expectations. Opinion polls show that most consumers are happy to have their personal information used for appropriate purposes if they are given an opportunity to "opt-out." The behavior of 132 million adults who took advantage of direct marketing opportunities in 1998 backs up these polls.

6. "Opt-In" will increase the burden of unsolicited calls. By requiring an explicit statement of permission prior to use of personal information, an "opt-in" system necessarily requires businesses to make extra contacts with consumers. The extra burden on customers will increase again if the absence of personal information increases mass mailings and telephone calls because businesses can no longer target their marketing only to customers who are likely to be interested.

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.)**

Voluntary opt-in essentially already exists, making legislative or regulatory action unnecessary. Financial institutions currently have the option of instituting an opt-in, and financial institution management should be allowed to continue to make this decision on a case-by-case basis without governmental involvement.

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.**

The ABA believes it is unnecessary and impractical to institute a provision in law or regulation to allow customers to opt out of affiliate sharing. Some financial institutions are voluntarily offering customers the opportunity to opt out of affiliate information sharing. Other institutions have concluded, due to cost considerations or other factors, to share information as allowed by law. Consistent with our observations regarding opt in, financial institution management should be allowed to continue to make this decision on a case-by-case basis without governmental involvement.

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?**

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

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

All of these questions essentially equate to an opt in and carry the same costs and considerations that are addressed in Question 8.