

Carl V. Howard
General Counsel
Bank Regulatory

Citigroup Inc.
425 Park Avenue
2nd Floor/Zone 2
New York, NY 10043
Tel 212 559 2938
Fax 212 793 4403



June 25, 2002

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

ATTN: Study on GLBA Information Sharing

Ladies and Gentlemen:

Citigroup apologizes for the delay in submitting this comment. Citigroup also respectfully requests the Department of the Treasury to include in the record this comment on the study of information sharing practices among financial institutions and their affiliates being conducted by the Department as required as part of the financial privacy provisions included in Title V of the Gramm-Leach-Bliley Act ("GLBA").

Citigroup has long recognized the importance of protecting the privacy and security of customer information. Prior to the passage of GLBA, Citigroup created its own self-imposed Privacy Promise for Consumers that we delivered to our individual customers around the world. With GLBA, Citigroup has delivered over 125 million privacy notices. These are in addition to our own programs, which we follow globally, and our privacy programs in each country where we have consumer businesses.

Citigroup believes that the study can be most effective if it is conducted with appropriate recognition of the overriding purposes of GLBA, the statute under which it is authorized, and with consideration of the substantial privacy developments since GLBA was enacted. The questions or topics for the study were developed more than two years ago and much has changed since then. Before addressing the topics presented by the Department of the Treasury in the second part of this comment, Citigroup presents certain additional factors that Treasury should consider.

For the record, Citigroup is a diversified global financial services company, the nation's largest registered financial holding company, and is subject to the supervision and regulation of the Federal Reserve under the Bank Holding Company Act. Citigroup and its subsidiaries

provide a broad range of financial services to consumer and corporate customers and have 192 million customer accounts in 100 countries. Citigroup engages in retail and corporate banking and asset management and trust services through ten insured depository institutions, including Citibank, NA. It engages in life insurance and annuity underwriting and a range of insurance agency activities through its Primerica and Travelers Life Insurance subsidiaries, and in securities activities through Salomon Smith Barney, a registered broker/dealer and a member of the New York Stock Exchange.

Part 1: Framework questions for the Privacy Study

1. Privacy should continue to be considered in the GLBA context of seeking to modernize the U.S. financial services industry.

A1.a. What impact did Title V ("Privacy") have on achieving the broader objectives of GLBA?

The overall goal of GLBA, initially entitled The Financial Modernization Act of 1999, was to streamline financial services, permitting financial services companies to offer a wider array of products and services at a lower cost to customers. Congress sought to accomplish this goal by allowing all types of financial services companies to affiliate, and by allowing these companies to cross market their products once they had become affiliated. Indeed, the House of Representatives Report (H.R. Rept. 106-74, June 15, 1999), reporting on the bill which later became GLBA, states (at p. 98): "The primary objective in allowing such affiliations is to enhance consumer choice in the financial services marketplace. . . ." The Report goes on to state (at p. 107): "H.R. 10 would create new opportunities for affiliations among different types of financial institutions, in turn providing an environment that will benefit consumers by enhancing competition, expanding the array of financial products available to consumers, increasing the efficiency of the institutions providing those products, and reducing costs to consumers as a result of this competition and efficiency."

Recognizing that affiliation and cross marketing would often involve the sharing of customer information, Congress included Title V in GLBA to provide basic protections for customers as the industry went through the expected rapid and massive change. While many financial services companies have not taken advantage of the new financial activities permitted to them by GLBA, all have had to meet the privacy requirements. Indeed, for many financial services companies, the major impact of GLBA appears to be the Title V privacy provisions.

The Department of the Treasury should consider the Title V privacy provisions in the context of other examples of laws, regulations and government directives that seek to balance privacy concerns with financial modernization in a manner similar to the aims of GLBA. In particular, the study should look at the EU Data Protection Directive that seeks to prevent privacy from becoming a trade barrier within the EU, the introduction of privacy notices on the Internet as a

way to build customer confidence, the role of privacy notices within the HIPPA Regulations to achieve more rapid automation of medical service delivery, and the role of fair information practices as a way of enhancing the accuracy of data for credit reporting under FCRA.

Treasury should also recognize that it is still early in the process to assess the effectiveness of the GLBA privacy framework. Financial services companies are in only their second cycle of notices under the privacy regulations. Moreover those regulations were developed in the limited period permitted by a mandatory statutory timetable. This was the first time U.S. privacy regulations were implemented on this scale.

Under the demands of this statutory deadline, the functional financial regulators cooperated to produce a largely consistent set of federal regulations. The process included a significant degree of interaction with and input from privacy advocates, the financial services industry and the public. We believe the openness of this process, the resulting consistency of the federal regulations and the level playing field among financial companies that has resulted, all argue strongly in favor of a federal privacy standard rather than a patchwork of state laws.

The agencies should be recognized for the level of cooperation and interaction that went into the drafting of privacy regulations. We feel that, in particular, the inclusion of substantial comment and discussion was positive and is something we would like to see in the development of future regulations and guidance.

Even with consistent federal rules, compliance with GLBA privacy requirement has been difficult and costly. Firms had to conduct company wide audits of information practices, implement changes to data and Web-based systems and internal control procedures, modify account applications and web screens, and review arrangements with outside contractors. In addition, notices had to be drafted to reflect the procedures and requirements of each major line of business. These efforts were not only time consuming but expensive for companies to implement. The direct costs for the preparation and mailing of notices and the indirect costs for the information audit, adoption of policies and procedures, negotiation of vendor contracts and installation of an audit/compliance system certainly cost the financial services industry over one billion dollars. Some companies may have decided not to share information simply because they did not have the resources to build an opt-out system in the allowed time.

The very real threat is that these costs will increase within the next few years as the states ~~hasten to enact more burdensome and restrictive requirements, centering on opt-in requirements and affiliate sharing restrictions.~~ These State developments threaten to make privacy compliance for national companies burdensome and costly and to undermine the very benefits of financial modernization that prompted passage of GLBA. There is a very real danger that State laws will severely erode such benefits as cross-marketing, a single centralized customer data base, centralized call centers staffed by third parties, single statements across business lines and uniform customer applications for varied financial products. Any comprehensive study should

evaluate the impact of the decision in Title V to allow the States to develop more stringent privacy requirements and the fragmented privacy requirements that result.

Of critical concern in preserving the benefits of financial modernization is the issue of the Fair Credit Reporting Act ("FCRA") preemption in the case of affiliates. Federal preemption under FCRA is expiring at the end of 2003. This impending deadline makes this study very timely. In particular, we believe that there will be major disruptions if federal preemption under FCRA is not extended.

In summary, this study should recognize that it is still early in the process to assess the impact of the privacy provisions of GLBA. Certainly the experts, in assessing GLBA's impact on anticipated consolidation and affiliation of the financial services industry, appear to agree that the immediate impact was less dramatic than anticipated and there will be a need to evaluate the results over time. The same should be true for the privacy provisions. In addition, the study should assess the privacy provisions in the context of the Act's overarching purpose of financial modernization. The preservation of affiliate information sharing and customer choice, are consistent with a clearly articulated privacy policy and measures to keep customer information secure. The balance of these objectives will permit financial services companies and their customers to achieve the benefits of GLBA. Finally, there is the need for consistent federal regulations that offer a national standard in place of a patchwork of State requirements.

A1.b. The sharing of information enhances the performance of financial institutions and results in better, less expensive service to customers.

Treasury is well aware of the challenges facing U.S. financial service companies, especially as separate industries migrate to a streamlined, integrated, and more customer-focused industry. For example the following facts have been noted in the media:

- Banks lose money on more than half of the accounts they serve and only begin to make money when a client has two or more accounts.
- Acquisition costs are rarely recaptured in the first year of an account; financial services companies only make money from longer and more stable relationships.
- Few companies can "manufacture" their own services in certain product lines which have significant scale benefits or which require special expertise. These may include broadly desired services, such as credit cards, or highly specialized services, such as high value tailored loans.
- Few financial service companies perform sufficient volumes of marketing across the full year to justify their own internal "plant" to create and mail their own offers. They may also be limited in their ability to develop, staff, and supervise a modern telemarketing center given the limited telemarketing done by most firms.

- Credit card companies are "on the hook" for credit costs whether through losses due to fraud, inappropriate customer selection, or bankruptcy.

In this environment, U.S. financial service companies are essentially compelled to meet a significant portion of customer needs through programs and products from affiliates and non-affiliated third parties. Any regulatory system that effectively prevents use of affiliate and third party resources will both curtail customer choice and increase the cost of financial services. Moreover, because of the nature of economies of scale, this lessening of choice and increase in cost will apply not only to customers who wish to limit the sharing of information but also to those who are unconcerned about information sharing. The benefits of information sharing that could be lost for all customers include exposure to a wider array of products and products directed to the particular needs of the customer, the convenience of one-stop shopping for multiple products, discounts for additional customer relationships, fraud prevention through knowledge of the customer, avoidance of multiple applications for each new customer relationship, and prompt updating of customer records to reflect change of address or other information bearing on customer service.

Most companies still capture information multiple times, as described below, for customers with multiple accounts. They experience costs in updating each of these separate databases when customers move. True financial modernization would involve a company using a common customer profile to deliver a broad set of products and services to meet a customer's needs. This may involve a single statement that consolidates information across accounts. This may be a single database where the information can be more accurately captured, validated, updated, and stored. This may involve a single point of access at ATMs and on Internet sites. It may involve a single financial professional who has appropriate licenses, training, and support to address the client's needs over a broad range of services. This would not only provide new benefits for the customer, but would do it at a lower cost than the current practice of separate statements, systems, and staff.

The concentration of credit card services in a few companies provides a good illustration of how the market may lead to a system that combines scale efficiencies with locally differentiated delivery. There are only a few major companies that process credit cards. Most other companies have found that they can go through these companies to offer a type of "private label" card to provide competitive services to their own clients. This results in better rates and services for the consumer as well as better efficiencies and products for companies.

Finally, with regard to this topic we endorse the analysis of how "Regulatory Structures Recognize the Benefits of Sharing Customer Information with Affiliates" in the Visa response authored by Rick Fischer, Oliver Ireland, and Obrea Poindexter of Morrison and Foerster LLP.

A2. The impact of U.S. privacy requirements on the globalization of financial services should be considered as part of this study.

A global framework is important to any study of privacy because financial service companies are increasingly active in providing services to customers across borders. Information sharing practices greatly differ around the world since these are driven by different histories and regulatory structures. It is noted that GLBA asks for a study of sharing among "financial institutions" without limiting the study to "U.S. financial institutions."

The U.S. is currently engaged in formal discussions with the EU as to whether the current requirements and regulation for U.S. financial service companies should be accepted as providing "adequate" protections for consumer privacy as defined by the EU directive. It would be helpful if the study considered the material gathered for these discussions. Also, the Canadian model has now been accepted as adequate by the EU and could provide a useful reference to look at practices in a country with a different regulatory history.

A3. Information sharing assists significantly in establishing strong relationships between customers and financial institutions.

Recent Congressional testimony pointed to the problem of "financial literacy" in the United States. Product choices have greatly expanded and the complexity of such products has also increased. Product complexity places a greater burden on individual consumers to make the right choices. Financial institutions with an ability to look at the full customer relationship may be able to help customers with these decisions. Examples of the assistance such information sharing permits include:

- Computer driven solutions, with automated messages on statements, at ATMs and on Internet services.
- Additional information for financial service professionals who have face to face meetings with clients and who can more directly ensure that consumers understand the advice.
- Invitations to the customer to attend appropriate seminars that may be conducted with the participation of other firms.

~~As many financial products are "sold" rather than "bought," the burden is on companies to effectively reach out to customers with products and services that are likely to meet short and long-term needs. Information from affiliated institutions can help companies take a fuller life cycle approach to offering appropriate products and services. This may be further expanded when a company can offer products from a wide range of affiliated and non-affiliated companies.~~

A relationship with a broker, banker, or insurance agent can be an important element in many people's lives. Such professional financial advisors understand customers' preferences and

product needs in a way that is too complex to be reduced to a series of "opt-in" and "opt-out" choices. The professional is expected to know if a customer would appreciate ongoing advice or invitations to customer events.

The challenge for financial modernization is to provide for privacy while still making it easy for the customer to have a meaningful relationship with a trusted advisor or institution. This advisor needs to have the ability to use personal information to best advance the interest of the customer, based upon the customer's profile, needs, and preferences. There is some point at which the client trusts the relationship manager to a degree that the customer allows that manager to use information to bring the customer an increasingly wider range of products and choices. For example, high-wealth clients, such as private bank clients, are likely to have an understanding, implicit or otherwise, that their banker or team may need to contract with many different product and service providers to meet the needs of the broad relationship. This is using information for the purpose it was given. The highly trained personal banker or team is expected to do what they can to advance the customer's interests. The reputation of the company and relationship with the customer depends upon appropriate actions. In this context, a series of "opt-ins" and "opt-outs" are likely to be viewed by the customer as an administrative burden or annoyance rather than as a protection.

This is also true for securities brokers, insurance professionals, and others who work in the financial services industry. The practical business considerations afford the customer more privacy protection than simple opt-in and opt-out programs and should be allowed to replace these when the relationship is long standing and under the control of an appropriately licensed professional. While there may be a broad level of consent, there may not need to be individual and distinct consent for every transaction or type of transaction. For example, the complex bidding structure that a broker may use to get the customer the best offer for an insurance product or mortgage may not be something that all customers want or need to understand in order to get a product that is only available through those methods.

As noted below in the request to reconsider the definition of "customer," even at levels below this "high wealth" area, customers and institutions consider the length and depth of a relationship in determining what is appropriate. For example, after experiencing good service for a period of time, customers may find it appropriate to hear about an expanded set of integrated products that may be available. Indeed, customers who do not get such a call from their banker, broker, or insurance agent are likely to feel that they are being discriminated against or that their business is not valued. ~~A paper path that tries to lock in each step of this developing relationship could effectively prevent such a relationship from occurring.~~

Moreover, the sharing of customer information among affiliated companies within this relationship is fully consistent with customer expectations. Holding companies often use common brands for their products and services so that consumers will understand that the holding company stands behind those products and services. In selecting a financial institution, consumers often do not understand that the various holding company activities are actually

conducted in affiliated companies, instead of in a single company. Typically, consumers expect that the branded entities are part of a single entity or are operating jointly. Accordingly, consumers expect that the information about them will be available for use and will be used throughout their financial institution and they are very often disappointed when one part of the corporation is not able to recognize them. For example, after the Citicorp/Travelers Group merger, many Salomon Smith Barney clients were disappointed when they were not recognized in Citibank branches, and vice versa. This is also confirmed by the low opt-out rates for affiliate sharing of consumer report information under the 1996 amendments to the FCRA. For these reasons, it is critical that GLBA continue to permit the sharing of customer information among affiliates.

A4. Privacy notices could benefit from a more customer-focused context.

Title V is based on the premise that the customer will have the opportunity to make an informed choice about the sharing of personal information on the basis of an effective privacy notice by the financial institution. Unfortunately, the complexity of the information to be contained in the notice, the excessive number of notices the customer is mandated to receive and increasingly the exceptions that must be included to accommodate individual State requirements have combined to make the notice less effective than it could be. The information presented at the recent Notices Workshop conducted by the FTC addresses the complexities of the notice issue, and the Department of the Treasury should take notice of the Notice Workshop materials.

As a result, one idea under consideration is a two or three tier privacy notice in which the customer begins with a short notice that addresses the items that are most likely to be of interest. The consumer would then have the opportunity to review more detailed privacy disclosures in a longer form notice that could be attached or available on a website, at the branch, or upon request. Consumer understanding of privacy notices could be further enhanced by having a single format for notices that applies both to financial companies and to non-financial companies.

There are many constructs outside of the U.S. for delivering privacy notices that do not involve the delivery of mail that some customers may find intrusive. In particular, the "public notices" in Canada provide extensive answers to questions but are only available upon request. The German model provides certain methods for providing notices through branches or other areas where the customer is likely to see them.

Finally, there should be more consideration of when privacy notices are given. For example, many products are opened via an agent or are otherwise outside of the context of the company who will have the relationship with the customer. There are auto loans initiated at a car dealer and then passed to an appropriate finance company or bank. Insurance products often trigger a notice requirement for both an insurance agent and an insurance underwriter. It may be more appropriate for a notice to be delivered with a welcome message that comes directly from the financial services company who will manage the relationship going forward. At that time, the

customer may be in a better frame of mind as to what privacy choices ("opt-ins" or "opt-outs") may be appropriate while they are making other operational decisions.

As an example of what might be changed to make the timing of delivery of notices more conducive to customer education and the formation of informed choices about privacy issues, Treasury should look at the current regulation's effect in the first mortgage business. Presently, the law and regulations require delivery of the privacy notice and opt-out choices at the "inception" of the relationship. In the mortgage context, this occurs at the closing table. However, at a mortgage closing, the consumer is presented with reams of paper, much of it mandated by one regulation or another. He or she is asked to sign document after document, and often, the lender is not in control of the process, since most loans are closed by independent title agencies or lawyers. As a result, it is unrealistic to expect that in all cases the privacy notice, as one document among many, is being fully read, explained and understood by the customer. Although the closing agent may advise the customer to take the privacy document home for study, we have seen instances where directions are not fully followed, and as a result, the customer simply signs and returns the document without making any privacy choices or with hastily made choices that do not reflect meaningful consideration. This reality does not serve the consumer or the industry well. Providing the company more flexibility in delivering notices within a reasonable time of the relationship opening may result in more meaningful choices. This would, as per current regulations, need to be done before the company could share information, including sufficient time for the customer to consider and respond to the notice.

The study may also discuss the purposes of privacy notices. While there may have been an expectation that GLBA notices would lead to a greater level of trust, they may have actually lowered the level of trust that consumers feel toward U.S. financial service companies, and U.S. companies in general. This is demonstrated in the tracking surveys done by Alan Westin and the Privacy and American Business organization as well as in other recent studies.

Part 2: Responses to the Specific Questions Raised

This section provides brief responses to the questions posed. In addition, we request that the authors of the Study reconsider two definitional issues, since they are material in shaping appropriate policy in this area.

~~**Customer/Consumer:**~~ The Department of Treasury Notice states that for the purposes of the Study, there is no distinction between a "consumer" and a "customer." This is contrary to both the Act and its regulations. For consistency, the Study should maintain the distinction between these terms and not treat them as "equivalents." Ignoring the distinction between "consumer" and "customer" also fails to take into account the relationship context that is so important in the banking, insurance, and securities industries. There often is a progression from "consumer" to "customer," as the company gradually wins the trust of the customer. Therefore,

the Study should recognize the distinction between "consumer" and "customer" as important for determining the appropriate level of information capture, use, disclosure, and sharing.

Nonpublic Personal Information: The GLBA regulations use a very broad definition of "nonpublic personal information" that, to many commentators, goes far beyond the actual statutory language of the Act to include virtually all information held by a financial institution, including the fact that a relationship exists. The Study may want to consider the impact of using this definition versus alternatives. Distinctions can be made as to different types of customer-related information. For example, there is commonly available information such as listed telephone numbers, information available from public records such as mortgage records, transactional information such as credit card statements, and information the customer might desire to have released upon specific request such as the fact that he or she is a deposit or brokerage customer. Many financial institutions would like to make a distinction as to how different types of information can be used and shared, recognizing that consumers do see differences.

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

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

We may share information about our experience with the customer and about the customer's transactions (e.g., account balance information; type of account (cash or margin); history of meeting margin calls). Experience and transaction information is shared with affiliates for a variety of reasons, including for anti-fraud purposes, institutional risk control, or as part of a referral made to an affiliate (with customer consent).

While financial service companies are quite conservative in sharing or disclosing information, it should be assumed that all information captured and held by a company may be shared with certain affiliates, as appropriate, at least by some companies.

There are affiliates in the same line of business created purely in response to State insurance regulation, slight differences in charters for depository institutions, and various licensing programs for financial service professionals. These may share account processing systems, customer service centers and databases to reduce the overall cost of servicing consumers. These ~~administrative/service activities may be conducted in an entity that is separate from each of the~~ line businesses it serves in order to enhance record keeping and cost allocation among affiliates, to meet tax concerns, to house jointly held licenses or patents or simply to accommodate internal reporting lines. A particular line of business, therefore, may consist of dozens of corporate entities, although both the customer and to a large extent the financial institution itself view the business line as single business unit.

There are affiliates in different lines of business that may share a common customer interface. For example, many financial institutions have joint employees who wear multiple hats. A single employee may function as an insurance agent, as a securities broker and a bank relationship manager. Customers are not likely to understand that restrictions on sharing information would mean that the person they talked to five minutes before in an insurance capacity is not allowed to remember and use the information received when they return to their role representing the bank or the securities broker-dealer.

Some organizations may be structured to use expertise within affiliates to perform particular roles, such as independent audit and legal functions, to develop and test operating systems, to develop and deliver marketing materials, to develop and deliver statements and bulletins, and for similar "doing business" purposes.

For cross-marketed or hybrid products, extensive legal resources may be required to define appropriate processes for the sharing arrangement. For example, when a licensed mortgage broker is brought in to help a private banker with a particular type of specialized product, a decision needs to be made about whether customer information should flow to the mortgage broker, to the private banker, or to both. This has little customer value but is done only to comply with information sharing regulations.

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

While financial service companies are even more conservative in sharing or disclosing information to nonaffiliated third parties, it should be assumed that all information captured and held by a company may be shared with certain nonaffiliated companies, as appropriate. While sensitive personal information, such as a social security number or bank account number may not be shared with a third party marketer, it may be shared with the third party data processor responsible for compiling and maintaining certain financial institution records.

One type of third party is someone associated with the customer, such as a family member, co-signer, account participant, beneficiary, guardian, neighbor, or potential signer for an express delivery package. Some of this sharing is appropriate, as indicated in the GLBA exceptions. In other cases, a financial institution may take great care to avoid unnecessary disclosures to this type of third party. Some of these types of sharing are governed by regulation; others are covered in the customer contract or in consent received from or disclosures given to customers. Some can safely be left to the discretion of the company. If companies abuse this discretion, they will lose their customers.

A second type of third party includes the many entities covered in the GLBA exceptions, such as auditors, legal counsel, other financial institutions necessary to complete a transaction, Federal and State regulators, credit reporting agencies, tax authorities, law enforcement agencies, and other necessary partners. For example, many third parties may be involved in completing a

mortgage transaction. With this type of third party, companies tend to share only what is needed for a particular transaction. Information provided to this type of third party is protected by professional or governmental codes of conduct, and/or by contractual agreements with strong confidentiality provisions.

A third type of third party is a person or company working under the direct supervision and control of the company, for example, temporary employees, consultants, and companies who produce operational or marketing materials. To some extent, these are companies that perform ordinary corporate functions that have been outsourced. Some of these, such as check printers and data processors, perform the same function for many companies. Others are dedicated to working with a single or small number of companies. These are, in effect, extensions of the company and must treat information in the same way the company would.

A fourth type of third party is a company with a specific contract in place for the provision of products and services. While the term "joint marketing" does not adequately describe the purpose and controls for this type of arrangement, this type of structure is necessary to maintain a level playing field between large companies who may be able to offer many products from their own family and other companies who need to draw upon partners to offer competitive products to their customers. Often these products are "manufactured" by a large company, such as one of the major credit card firms, and sold by smaller institutions. There are many different appropriate models, including those where the large company owns the products but allows customer benefits to flow through to the partner, those where the smaller company owns the product and pays for the "servicing," and even cases where the ownership is passed through to the financial markets with the larger company processing and the smaller company maintaining the relationship.

A fifth type of third party relationship arises when a company, portfolio, or individual account is sold or transferred to another party. For example, delinquent credit products may be sold to a company that has expertise in collections or workouts. Portfolios may be sold to another company with or without the servicing responsibilities. Portfolios may be sold to the financial markets as a purely financial transaction. In some cases, the company may simply reorganize under a different name or expand/contract the number of affiliates for appropriate business purposes.

A sixth type of third party is an independent company that has an offer it would like to make to another company's customers. ~~GLBA regulations apply whether the mailing list is delivered to the third party or the mail is sent by the institution itself, with replies going to the third party.~~ Recent OCC bulletins on web-linking and third party relationships cover many other structures and address the risks connected with this type of offer.

While the Treasury Study may look across industries, examples from particular types of companies can be instructive. For example, a broker-dealer may share information with

nonaffiliated third parties in the process of servicing and administering a client's account in a variety of ways.

- Information about mutual fund shareholders (e.g., the customer's name, social security number, and number of shares owned) must be provided to a vendor to make various fund mailings, including sending proxy statements and prospectuses, to the fund shareholders.
- For those clients who own limited partnerships, information about limited partners is provided to the partnership's general partner (with client consent).
- Information about retail customers who own shares of stock is shared with a vendor, so that the vendor can disseminate a company's annual report, quarterly report, or interim report to shareholders. In the context of a proxy fight, a third party/solicitation company will purchase from the vendor the names of the non-objecting beneficial owners of a company in order to contact the customer to vote a particular way.
- If a customer requests that a physical stock certificate be issued in his or her name, instead of shares being held in "street name," the third party transfer agent must be contacted and instructed accordingly. To implement the instruction, the transfer agent must have the relevant customer information. Then, the physical stock certificate is mailed to the customer.
- Information required in response to a subpoena, or court order.
- Information requested by law enforcement agencies.
- The Depository Trust Clearing Corporation (DTCC) is provided, on a daily basis, client names, addresses, social security numbers, and number of shares owned in a particular company. DTCC uses this information to facilitate a customer transferring a specific stock, or an entire account, out of one firm to another, or even to the client.
- On an annual basis, we provide to individual States the name, last known address, social security number, and amount of monies/securities in certain accounts, for purposes of compliance with their escheatment and abandoned property laws.
- ~~In addition, sharing of information may be required to comply with various other state or local laws or regulations.~~

1.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.

It depends on the purpose of the sharing, as illustrated by the discussion above.

First, there is a better opportunity to assess and ensure the practices of an affiliate in terms of information security, use of information, and other privacy matters. Almost by definition, controls should be better with an affiliate, policies should be consistent and knowledge of those policies easier to assure.

There are likely to be more consistent practices among affiliates allowing for easier and less risky interfaces, such as for transporting and displaying data. For example, shared customer service screens have security entitlements that control what each individual sees. These types of screens may help validate the identity of a customer who is attempting to open a new account or to perform a particular transaction. This is difficult to do with third parties. It also should be noted that a company may have policies for sharing among affiliates in the same line of business that are different from their policies for sharing with affiliates in other lines of business.

The customer often benefits from services that combine product features from different affiliates, for example, a mortgage backed by securities held at the brokerage affiliate. Therefore, the customer is less surprised when their data is in a shared database and on joint statements from a family of companies. In fact, many customers appear to prefer this combined approach so that they do not need to give the same information repeatedly and do not need to receive and examine a large number of separate account statements.

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

Financial institutions may share information with affiliates as permitted under federal and state laws and regulations (e.g., to combat fraud, money laundering or suspected terrorist activities). They also may share information in connection with credit decisions or for cross-marketing purposes, in order to offer a client a new product or service. Affiliate sharing may offer the customer an opportunity to use an affiliate's product that the client was not aware of, or offer a customer a more competitive rate for that product or service than the customer was receiving from a nonaffiliated third party.

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

This has been addressed in the responses to 1a-1c above.

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

Financial institutions may place contractual limitations on the sharing of information (e.g., confidentiality clauses, restrictions on re-use, information security, right to audit). Also, for information shared with affiliates, there may be interaffiliate agreements that limit use of the information. Affiliates may not be able to use information to gain a benefit outside of the specific use that is agreed to in an "arms length" negotiation. Non-affiliated third parties would

have similar restrictions designed to protect customers' privacy and company's intellectual property, and to enforce information security and performance standards.

Historically, financial companies impose tight restrictions over the sharing of information about customers due to the fact that information is considered to be one of the most important assets of the corporation. There are intellectual property rights to the data that must be protected. The company may choose to litigate with those who attempt to steal customers or their information. Even within a larger financial services company, it is a normal practice for each affiliate to carefully guard the information it has about its customers.

In addition, the FCRA places conditions on using information that is not the direct experience of the company. Financial institutions have to limit certain information shared with affiliates and with non-affiliates to be compliant with the FCRA. In other cases, the company cannot prevent sharing information when, for example, it must be provided to law enforcement agencies or to credit reporting agencies.

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

Even within a financial holding company, each business wants to protect the individual customer relationships it has established. Again, this information is of great value to the corporation. Agents, brokers, and other staff want to control the flow of data concerning their customers and do not easily give up control of information to others.

1.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?

This may be better seen in contrasting the practices of U.S. financial services companies with those of some institutions outside the U.S. Ideally, an institution would like to have a full picture of its customer, offer products at each life stage to meet the customer's needs, protect itself and the customer from fraud, and follow the customer as the customer moves geographically or to new careers or to levels of increased financial responsibilities. The complexity of laws, regulations, and corporate structures in the U.S. makes this type of integration difficult, but it would greatly cut customer acquisition and attrition costs and could also lead to a better match of customers to products.

Regulations, such as those under FCRA, also limit the sharing of information in ways that may hurt companies. For example, since FCRA does not have exceptions to the same degree as GLBA, it may prevent information from being shared for certain anti-fraud programs. This may result in a greater burden on companies and consumers both to understand why such information cannot be shared and to actually prevent the fraud. It also complicates the preparation of notices that need to comply with these "apples" and "oranges" regulations in one place.

One use that clearly needs an exception is to prevent funds from becoming abandoned. A financial institution should be permitted to publish depositor names in the paper, or make telephone calls and other contacts to give notice and permit the depositor to claim his funds. This is a normal course of business use, and much in the interest of customers.

A similar use is to claim funds when a failed depository institution is acquired from the FDIC or other insurer. There is only a short period of time, perhaps 18 months, for the acquiring institution to contact all of the depositors of the failed institution in order to obtain ratification of their accounts. This is a formidable task, which requires newspaper ads, direct mailings, and telephone calls, done at a time when the institution's own personnel are swamped with other work from the acquisition. Being able to share customer information and use whatever means necessary is critical not only to depositors (because otherwise they will lose their funds to the insurer) and to the acquiring institution.

A proposed acquisition is another situation where customer information must be shared. Whether only a portfolio or an entire institution is being acquired, the due diligence and pricing process necessarily involves any proposed acquirer having at least some access to customer information that might otherwise not be allowed to be shared. This was appropriately included as an exception in GLBA, and should be retained.

In addition to these specific examples, longer term, it would be good to work toward a concept that an exemption is needed for any situation in which the customer clearly is benefited by such sharing (for example, by not having to fill out all new paperwork when an account is opened). This would address a structural flaw of GBLA in that it talks only about sharing (rather than about contacting the customer for marketing purposes when the customer doesn't want to be contacted), and appears to have an assumption that sharing will harm the customer. In fact, customers normally want the institution to use their information in any way that clearly brings benefits to them. They are not likely to understand situations where the institution fails to contact them to bring benefits or prevent harm due to overly restrictive rules on sharing information.

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

2.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.

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

2.c. Do existing statutory and regulatory requirements protect information adequately? Please explain.

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

We believe that the current guidelines for information security as well as other related guidance on third parties are both adequate and appropriate to financial institutions. Given the rapid changes in technology and management solutions in this area, the federal banking regulatory guidelines for information security provide a more positive and flexible solution than would regulations that lock in practices that are good only for a short period of time.

It may be inappropriate in a public document to detail the information security programs that companies have in place. However, these are being reviewed in detail as a result of scheduled information security audits by federal banking regulators covering the GLBA guidelines. These reviews will address the procedures in place in each institution to determine whether policies and procedures are appropriate to the risks faced by that institution.

Most institutions have extensive manuals and training programs to ensure the security of their information. These protections may include firewalls, encryption and other new technology since availability of technology may be more important than statutory and regulatory protections.

However, there is still some tension with respect to vendors who handle such information but are not themselves financial institutions, such as e-commerce vendors and other new companies. In this respect, the FTC rules on GLBA information security are still unsatisfactory, as pointed out in other comment letters since they provide for ~~FTC enforcement against vendors contracted by regulated entities~~. Traditionally, the federal banking agencies have had this enforcement role recognizing the vendor as an extension of the company.

Most important to us, the FTC proposed rule is inconsistent with other GBLA information security regulations. It is also inconsistent with well-established and effective regulatory structures and practices (e.g., that the OCC regulates national banks and national bank subsidiaries).

The FTC's proposed rule also does not reflect the concept, common in the EU, of a "data controller." This means that the requirements for protecting information should travel by law or regulation with the information. Whoever has the information should have to protect it to the same high standard that applies to the financial institution whose information it is. Permitted use would be restricted to use permitted by the financial institution under contract with the third party.

In other words, as a condition of a vendor performing specialized services for a financial institution, the vendor should be bound, by law or regulation (and not just by difficult contract negotiations), to the same standards for privacy and information security applicable to the financial institution. The vendor should also be subject to audit by the financial institution and examination by the financial institution's regulators.

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

3.a. What, if any, potential privacy risks does a customer face when a financial institution shares the customer's information with an affiliate?

We recommend that Treasury also consider the converse risk, namely the impact on privacy where the financial institution is not allowed to share information with an affiliate. Stale, missing, or inappropriate information may prevent companies or their customers from taking the following types of actions:

- Providing customers investment choices based upon an appropriate risk profile when the customer has little time to provide such information or where the customer chooses to provide inaccurate information.
 - Being able to update addresses, phone numbers and other significant changes across all accounts even where the customer only provided the information on a select number of accounts.
 - Properly identifying an applicant for an account, service, or transaction, in a way that picks up prior credit problems and criminal activities both within the same family of companies and from other relevant and accurate sources.
-
- Enabling the customer to more easily recognize problems reported on statements due to a reduced number of statements the customer receives. For example, with fewer, more consolidated communications, the customer may more easily notice when statements stop arriving unexpectedly (i.e., are compromised via an unreported change of address)

3.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?

Since third parties may be more likely to have different standards, this may lead to somewhat higher risk levels. For example, the risks identified in response to 2.d. above apply. These considerations would argue for a framework that:

- Makes it easier for financial companies to include appropriate clauses in contracts to ensure that vendors treat the information in as secure and private a way as the financial company itself.
- Ensures that vendors do not have a financial advantage in being able to perform tasks in a cheaper way due to standards that are more lax in such areas as privacy, security, redundancy, continuity of business, etc., -those "intangibles" that make a financial institution more trustworthy, but that do cost money to implement.
- Ensures that appropriate functional regulators enforce privacy regulations for the regulated entity, its subsidiaries, and its vendors as has traditionally been the case for federal banking agencies. These agencies can promote consistency of regulatory approach and have the ability to inspect and examine for compliance most efficiently because of their knowledge of particular institutions and the functioning of the industry.

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

Under FCRA, information received from an affiliate is not considered to be the direct transaction or experience of the institution. Therefore, FCRA limits the disclosure of this information as "other" information. This appears to be driven by the fact that such information was seen as having a greater chance of not being accurate.

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):

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

FCRA, in particular, points to the benefits of broad information sharing. It is generally accepted that customers can borrow at significantly lower interest rates in the U.S. as a result of the information sharing facilitated by the FCRA. These benefits have been addressed in various reports that contrast U.S. markets and other global markets in the penetration, pricing, and competitiveness of credit products. This is largely due to the fact that FCRA encourages and facilitates more accurate, standard, and timely information for making credit decisions.

The accuracy of data, which comes from information sharing, is also a benefit in many other areas where the institution interacts with the customer in face to face or remote transactions. These include quick and accurate identification/verification of the customer, paperless transfers among accounts, and reduction in "nuisance transactions", such as bounced checks. Information

sharing has a tremendous benefit for anti-fraud purposes since it is used to detect and prevent potential fraud against the company and its affiliates.

These benefits occur at several times throughout the relationship, including the opening of new accounts. Information sharing may reduce the cost by upwards of \$100 per account opening because the necessary information is on file. It also may prevent the costs associated with customer attrition, and it may smooth any change in customer lifestyle such as a marriage, divorce, move, birth of a child, or other event that causes a new evaluation of financial needs.

Information sharing with affiliates can provide clients with the opportunity to learn about products and services offered by another affiliate that may provide specific benefits (e.g., insurance, credit cards, loans, and banking). Since the information has already been captured by the affiliate, sharing is an easy and fast way for customers to learn about potential products of interest. In addition, since the cost to the company may be less, these products or services may come with special fees, rates, or features that are not available to non-consolidated customers.

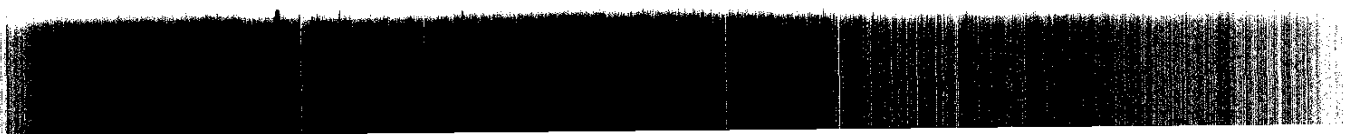
Information sharing may, in fact, be necessary for the creation of certain new products such as those that combine components of a mortgage and a brokerage account. This can give companies a competitive advantage, since they can compete by creating and offering specifically designed products rather than by simply competing on price with generic offerings.

Sharing information may allow the company to offer an appropriate product rather than to simply turn down a consumer who has applied for an inappropriate product. Since a large number of credit applications result in a denial, the company can recoup some of its processing costs if it can offer the consumer a product from an affiliate that would be more suitable for the customer or for which the customer would qualify.

This sharing also has important operational benefits for institutions and their customers in the form of combined statements and consolidated ATM screens, internet banking, and call centers. By storing the information once and using it across the institution, the company is likely to reduce costs of updates and maintain more accurate information for each account. Since a sales person would see the consolidated information, he or she would be in a better position to understand the customer and talk about current and future needs.

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

Most financial institutions in the U.S. do not have the resources to offer all products themselves. To pick an example, most financial institutions that nominally offer credit cards in fact partner with a few large card issuing institutions to offer credit cards under the brand name of the first company. Therefore, all of the benefits described above could potentially be available through associations with nonaffiliated third parties.



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

The U.S. is home to a broad range of affiliate structures. Some of these affiliates specialize in "manufacturing" products, others may specialize in distribution, and still others may specialize in operational efficiencies. By working together, each affiliate can focus on what it does best and also have a ready channel for products, distribution, and other elements that it does not have. Banks learned this lesson when inter-state banking restrictions caused segmented customer service facilities dedicated to one bank subsidiary to be idle while customers at other bank subsidiaries suffered long waits. Significant operational gains have been made possible simply from being able to cross-train, license, and employ staff to service various affiliates.

As another example, when a customer applies for a mortgage via phone from an institution where the customer has an existing relationship, the company may -- with the customer's verbal permission -- be able to gather all of the information needed from internal sources, greatly cutting time and expense for the institution as well as the customer. This may also reduce abandonment rates, increase the accuracy of the information, and allow the institution to promise a much faster closing date.

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

This is restricted due to the fact that this is "non-transactional and non-experiential" information under the FCRA. If the FCRA were amended, such information sharing may have significant anti-fraud benefits.

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

Given that financial services run on information, this would potentially "knock out" competitors who now rely on affiliates or third parties. This may result in a major restructuring of U.S. financial service companies into a small number of large and integrated institutions, such as are seen in other countries. While there would be room for boutique and specialty firms, medium sized companies would not be likely to survive against those with better efficiencies, broader offerings, and better integration. Even though Citigroup may benefit, we consistently ask for a "level playing field" so that the market decides what is appropriate, not laws written in particular ways that favor one player over another.

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

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

Commentators often assert that American consumers do not do a very good job of either understanding their financial needs or acquiring appropriate products and services. Therefore, one of the most important benefits of information sharing for consumers is the greater possibility of companies understanding and assisting consumers to meet their needs over a period of time with a diversity of products. For most financial companies this will require working with affiliates or third parties.

Conversely, to the extent that each customer needs to individually shop for and purchase these products, information sharing can help bring the consumer products that better match their needs if they are available through an integrated set of product offerings at the selected institution. Without this "one stop" approach, many customers would go without important products or protections.

Consumers also benefit from fraud prevention programs that come from better information. While credit card companies may absorb the direct cost of credit card fraud, consumers may still have significant expense in getting their lives back together. Fraud prevention is also very important for other types of accounts, such as insurance, banking, and brokerage.

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

The answer here is the same. Products that could potentially be bought through an affiliate could also come from a trusted third party. To the extent that the third party has a better or more suitable product, the consumer would benefit. Here, the limits on sharing information for fraud-prevention purposes may be overly restricted due to FCRA provisions that were established many years ago.

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

~~This type of sharing is expected to be very rare, for reasons given in 4.d. above.~~

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

We do not see any alternatives to the approaches described in 5a and 5b above that are equally beneficial since they would require customers to provide the same information to each institution and go through multiple versions of the same sales process. Unless the customer is

willing and able to share information about all accounts, the fragmented advice that will result is likely to be less sensitive to the customer's actual situation and needs.

However, as a result of GLBA, more companies understand the special needs of customers who value privacy more highly than convenience or even price. This is resulting in the testing of new products and a greater emphasis on developing and communicating privacy choices that can make these customers more comfortable providing information, especially in the electronic environment. These programs are in the early stages and may be expected to develop over the next few years. Premature regulations are likely to reduce the probability that companies will develop the best products and services for this group since they will be hampered by the regulations.

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

New barriers and limitations are likely to result in significantly poorer and more expensive service and advice. This may lead to inappropriate investments, inappropriate mortgage and other credit product selections, and significantly higher fees for checking and savings accounts. If customers are not willing to go through the resulting inefficient process to buy these products and services, they may go without many beneficial services.

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

6.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.

GLBA and FCRA provide extensive protections for customers. GLBA, in particular, strikes the right balance between protecting customer privacy and ensuring that customers receive the benefits of financial service affiliations and related cross marketing. Beyond this, it should be recognized that the privacy programs of U.S. financial service companies are driven by the desire of companies to build trust and long lasting relationships. This means that even before GLBA, most companies had policies and standards that were significantly higher than those mandated by law.

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

A single national consumer privacy law is highly desirable. At minimum, FCRA needs to be revisited in 2003, before the exceptions for sharing information with affiliates expire at the end of the year. This also would be an opportunity to make a small number of changes to allow GLBA and FCRA to work together in a more seamless fashion, such as by adding GLBA type exceptions to FCRA. There could also be consideration of uniform privacy laws covering all industries, rather than only financial services.

It may also be recognized that the initial and annual privacy notices mandated by GLBA may not have had the desired effect. Therefore, these notice requirements should be reconsidered. The type of "public notice" available from Canadian companies may be considered as preferable in addition to a short notice sent to consumers. While a shift to such notices would require significant effort and expense by companies that have just gone through a similar exercise to implement GLBA, this may be justified if use of such notices created greater uniformity with non-financial companies.

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

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

Although the GLBA privacy notices used by most financial institutions have been adequate in meeting the complex requirements of the statute, they may not have been completely satisfactory from a customer point of view. Companies have received very few direct comments or complaints from customers, but some would argue that GLBA privacy notices may contain too much information for the ordinary customer to review or understand. It should be noted that prior to GLBA, voluntary privacy notices, such as those from Citigroup, were well received and widely praised for clearly stating company policy. These were often driven by needs that were expressed directly by the customer. Part of the issue may be that an individual consumer may be bombarded by dozens of such notices from each of his or her financial institutions and part of the issue may be the need to address the complexity of GLBA itself. In addition, the notices must be provided to the consumer and not merely posted at the offices or on a website for the consumer to peruse.

By forcing companies to provide notices on an aggressive time table, these notices may have caused some companies to stop beneficial information sharing, since they may not have had time to create an opt-out system. Others may have found it hard to explain the benefits of information sharing within such an already lengthy notice.

7.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.

One avenue to explore would be a brief privacy notice that addresses the most important elements for the consumer. Such a short form notice would have to be accompanied by the full GLBA notice unless GLBA is revised to allow financial institutions to refer customers to a more detailed notice. The cost of moving to a short form notice regimes, however, should not be ignored. Such a notice may result in a need to revise virtually all account opening materials. Any change to a short form GLBA notice would be made significantly more difficult if it has to

include multiple and differing State law requirements. Finally, any change to the GLBA notices would have to accommodate the conflicting notice requirements of GLBA and FCRA.

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:

8.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 consumers.

Opt-ins and opt-outs provide similar consumer protections in that both are based on consumer choice -- in each case, the customer chooses the preferred privacy alternative. Opt-ins, however, involve a significantly greater cost and compliance burden for the companies that must comply with their requests. In a free market, the proponent of a regulatory burden is normally expected to demonstrate why the burden is justified and why a less burdensome remedy could not be used. Here, an opt-out is a much less burdensome remedy that provides a very similar opportunity for consumers to express their privacy preferences. Moreover, opt-ins are especially hard to justify with regard to affiliates because most consumers do not focus on separate legal entities within a family of companies. Rather, they generally assume that they have a relationship with the entire family.

8.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 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.)

Allowing free markets to resolve issues regarding the terms under which goods and services will be provided is generally the most efficient method of resolving such issues. Government should operate with a presumption that market forces are preferred over regulation unless the proponents of regulation demonstrate that market forces will not resolve an issue and that the proposed regulatory remedy is the least intrusive type of regulation that will resolve the issue. We believe government should encourage voluntary solutions to most issues. An opt-in provision is such an intrusive remedy, when compared to a privacy notice and opt-out based remedies, that Citigroup believes an opt-in requirement (as opposed to voluntary actions by financial institutions) can only be justified in rare circumstances.

In Citigroup's experience, there is a broad middle ground of consumers who are not so significantly engaged with the issue of privacy that they will take action on either side of the issue. They will not opt in and they will not opt out. In a free market economy, the question must be asked whether financial institutions should bear the administrative burden of convincing the

customer to become engaged and make a privacy decision? The customer is provided with a clear statement of the financial institution's policy and with the customer's remedies to restrict the sharing of information. It is the customer's decision whether to invoke the remedy, and the financial institution should not be penalized for the customer's inaction.

8.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].

Citigroup and its predecessor organizations have had a voluntary opt-out program in place for over fifteen years with regard to the sharing of information for marketing purposes. This has been well accepted by customers since it allows the choices to be directed by what the institution hears from its own customers and can be provided in language that makes sense to the customer base.

The answer to this question may be different when information sharing is done for different purposes, such as risk control, operations, and marketing.

Where the customer does not want information shared for normal types of risk control, such as credit or fraud risk, companies may avoid doing business with the customer.

This may also be the case where sharing information is done for operational reasons, such as to reduce costs and increase the accuracy of information. As companies consolidate their operations, they may not be able to serve customers who will not allow their accounts to be housed on a common database since that may be their sole means of operation.

Use of information for marketing may be considered a special area. In looking at financial service companies (in contrast with companies in other areas), it should be recognized that financial service companies generally provide offers directly from the company or person who has the established relationship with the client, since this has proven to be much more effective as a marketing and sales approach. While this person may control the relationship, there may be necessary referrals to affiliates or third parties due to other regulations and licensing requirements for specific products and services.

8.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.

The comments above would also apply here. There are many current opportunities, such as the opt-outs provided by the credit reporting agencies, opt-outs under the Telephone Consumer Protection Act and State Do Not Call lists that may still not be well understood or used.

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:

9.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 information may be shared?

Many companies needed to quickly develop opt-out systems to meet the tight regulatory deadlines. However, more interesting pilots of customer relationship management programs are beginning to develop more satisfactory methods for offering privacy choices in a more customer friendly manner. As technology progresses, companies are likely to invest in such systems both for the resulting cost savings as well as for their impact on customer satisfaction.

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

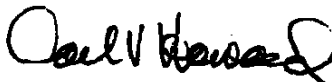
A program that integrates these choices with fuller uses of customer information would support the goals of financial modernization. These customer-focused approaches take years of trial, error, and innovation to develop and mature. To the extent that these are imposed from a theoretical framework, they would not be expected to work. Therefore, any imposed policy that scripted these dialogues would be likely to delay advances rather than make them move faster. For example, the customer focused privacy notices done before GLBA were widely praised while the theory driven notices required by the Act did less to advance privacy communications or protections.

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

A survey of financial institutions may show that many institutions greatly cut back on programs of this type as a result of the GLBA privacy requirements. This may have been due in part to the redirection of resources to develop the systems and notices required by GLBA. It may also have been in response to the negative impact that required GLBA notices had on the trust consumers have for financial services companies. While this may not have been Citigroup's experience, such developments have been the subject of discussions in public seminars and other forums.

If you require additional information, please contact James Scott (212-559-2485, scottj@citi.com) or Steve Durkee (212-559-2144, steve.durkee@citicorp.com).

Very truly yours,



Carl V. Howard