

27A

May 10, 2002



**Via Hand Delivery**

Regulations and Legislation Division  
Chief Counsel's Office  
Office of Thrift Supervision  
1700 G Street, NW.,  
Washington, DC 20552  
ATTN: Study on GLBA Information Sharing

Re: Comments on the Gramm-Leach-Bliley Information Sharing Study

Ladies and Gentlemen:

This comment letter is submitted on behalf of Visa U.S.A. Inc. ("Visa") in response to the request for comment pursuant to section 508 of the Gramm-Leach-Bliley Act (the "GLB Act"), which requires the Secretary of the Treasury ("Secretary"), in conjunction with the federal banking agencies, the Securities and Exchange Commission and the Federal Trade Commission ("FTC"), to conduct a study of information sharing practices among financial institutions and their affiliates ("Study"). To assist in the preparation of the Study, the Secretary issued a request for comment on a number of issues relating to information sharing, as well as on broader issues regarding financial privacy. Visa appreciates the opportunity to comment on this important subject. Visa has already submitted a comment letter focusing on the affiliate sharing aspects of the Study, and is now submitting this comment letter to address broader issues relating to the privacy of consumer financial information more generally.

The Visa Payment System, of which Visa U.S.A.<sup>1</sup> is a part, is the largest consumer payment system in the world, with more volume than all other major payment cards combined. Visa plays a pivotal role in advancing new payment products and technologies to benefit its 21,000 member financial institutions and their millions of cardholders worldwide. Visa and its members have a keen interest in issues relating to the use and disclosure of consumer information.

To private sector parties, issues involving the uses and disclosures of customer information require the balancing of the economic efficiencies that result from the dissemination of consumer financial information and the privacy interests of individuals that are rooted deeply in the American culture and legal system. This

---

<sup>1</sup> Visa U.S.A. is a membership organization comprised of U.S. financial institutions licensed to use the Visa service marks in connection with payment systems.

balancing of economic efficiency against privacy interests is not new. Congress was required to consider these same competing interests in adopting the Fair Credit Reporting Act ("FCRA") over thirty years ago. Visa believes that these competing interests can and have been reconciled, both in the FCRA and more broadly, and that consumer expectations for the privacy of financial information generally are being met today. However, Visa also believes that other privacy issues, including issues relating to government access to information, telemarketing, and identity theft, are often confused with the issue of the disclosure of information about consumers to private parties. Rather than engage in a semantic debate about the meaning of privacy, this comment will identify the issues relating to the disclosure of consumer information between private parties ("Information Sharing"), evaluate the current state of these issues, and consider additional steps that might be taken to remedy perceived problems.

### **PRIVACY AND EFFICIENCY**

In evaluating Information Sharing practices, it is critical to recognize that privacy interests cannot be viewed in isolation--that is, personal privacy as it relates to financial information is not an absolute value that outweighs all other interests. First, all consumer financial information ultimately relates to transactions or relationships between the consumer and other parties. These other parties also have an interest in this information because these transactions or relationships involve them every bit as much as they involve the consumer. Nevertheless, perceived discrepancies in bargaining power, coupled with concerns that traditional, although sometimes unexpressed, expectations as to the confidentiality of information may be eroding with improvements in telecommunications and information processing, have led to a concern that consumer financial information may be used by financial institutions in ways that consumers do not expect and would not endorse. These concerns have led to the current examination of whether the interests of the parties to these transactions have been appropriately balanced by the GLB Act and other requirements, or whether further action is necessary.

In conducting this examination, it is important to recognize that there are larger issues at stake than the interest of the parties in individual financial transactions. Information Sharing is a critical component of economic efficiency and the gains in productivity that spurred much of the economic growth of the late 1990s. As Federal Reserve Chairman Greenspan stated in a letter to Congressman Markey in the summer of 1998, "Detailed data obtained from consumers as they seek credit or make other product choices help engender the whole set of sensitive price signals that are so essential to the functioning of an advanced information based economy such as ours." A year later, in testifying on financial privacy issues, Governor Gramlich echoed these views stating that "Information about individuals' needs and preferences

is the cornerstone of any system that allocates goods and services within an economy. The more information about needs and preferences that is available, the more accurately and efficiently will the economy meet these needs and preferences.”

The link between Information Sharing and economic efficiency is not difficult to understand. If a provider of goods or services understands what its potential customers need and want, it will not waste money developing and attempting to sell those customers products or services that they neither need nor want. And, competitive pressures will lead to some or all of the resulting savings being passed on in the form of lower prices to customers, enabling those customers to acquire other products or services with their savings, and thereby to enjoy higher economic standards of living. In addition, the ability to tailor products or services more precisely to consumers' needs and wants and to bring offers of those products and services directly to the consumers that are most likely to choose them, saves consumers search costs and time, and avoids the inconvenience of consumers searching for appropriate products and services on their own. Thus, Information Sharing contributes both to higher economic standards of living and to a higher quality of life though increased time for discretionary and leisure activities.

Individual consumers have long recognized these benefits in their own choices by repeatedly dealing with favorite providers of goods and services. Although some of these repeat transactions represent a preference for the inherent quality or price of the goods or services, many repeat transactions represent the consumer's recognition that the provider understands the consumer's particular needs and preferences. Thus, consumers regularly do business with neighborhood businesses because of their greater understanding of what consumers need and want. Improvements in technology have increasingly allowed large national businesses to provide these same benefits to consumers. Although the mechanism is different in substance, Information Sharing by financial institutions is done for the same reason that neighborhood businesses remember their customers' past transactions, so that the provider or recipient of the information can serve the customer better. Although the disclosure of information to third parties may be viewed as injecting privacy concerns into these transactions, so long as that sharing is conducted within the scope of the customer's expectations, privacy concerns do not arise.

While neither the benefits of Information Sharing nor privacy interests are readily quantifiable in economic terms, recent studies suggest that the benefits of Information Sharing are substantial. For example, a study by Ernst & Young, *Customer Benefits from Current Information Sharing by Financial Services Companies*, dated December 20, 2000, that was commissioned by the Financial Services Roundtable, estimated that information sharing saved customers of the Roundtable's members a total of approximately \$17 billion per year. Another study

by Dr. Peter Johnson and Robin Varghese, *The Hidden costs of Privacy: The Potential Economic Impact of Opt-In Information Privacy Laws in California*, dated January 2002, commissioned by the California Chamber of Commerce, estimated that opt-in restrictions on third-party information sharing in California would likely cost California consumers, employees, and taxpayers billions of dollars. In addition, such restrictions would likely cost California charities \$1.57 billion in lost revenue. Similarly, a study by Michael A. Turner and Lawrence G. Buc, *Impact of Data Restrictions on Fundraising for Charitable & Nonprofit Institutions*, dated January of 2002, estimated that opt-in third-party data sharing would cost charitable organizations \$10 billion in direct mail and telephone solicitation costs. Other studies note that Information Sharing is closely linked to the availability and price of credit. For example, credit is less available and where available, available only at a higher price, in countries where Information Sharing is less highly developed than in the United States.

Finally, at the same time that improvements in technology are increasingly permitting customer information to be used to promote economic efficiency, these same improvements, as well as market developments, are permitting businesses to refine their needs for information. Businesses are increasingly able to act on less, but more refined, information, thereby minimizing disclosures of customer information. For example, modeling and marketing that were previously done by a third-party seller may now be done by a financial institution itself, with the result that the only information received by the seller is the identity of those financial institution customers who actually elect to acquire that seller's products or services.

#### **SEPARATE INFORMATION SHARING FROM GOVERNMENT ACCESS TO INFORMATION, TELEMARKETING, AND IDENTITY THEFT**

In evaluating Information Sharing practices, it also is critical to recognize the true relationship, or lack thereof, between Information Sharing within the private sector and the related, but distinct, issues of government access to information, telemarketing, and identity theft. In this regard, it is important to note that perceptions of consumer concern about the privacy of financial information appear to differ widely. Although various surveys report a high level of consumer concern about the issue of privacy, focus groups used by depository institutions to help them analyze their approaches to complying with the GLB Act suggest that most consumers have a high degree of trust in their banks' use and protection of information about them.

Further, while it may be argued that the low opt-out rate experienced by financial institutions that offered their customers the opportunity to opt out of disclosure to nonaffiliated third parties in their GLB Act privacy notices is due to a

lack of understanding by consumers of these notices, this view is difficult to support. The blizzard of notices directed at consumers in the spring of 2001 did not go completely unnoticed. Secondary sources ranging from local newspapers to national television networks, as well as consumer advocacy groups, called attention to these notices. If consumers had a strong interest in opting out of Information Sharing, it is hard to imagine that opt-out rates would not have been significantly higher than the few percentage points experienced by virtually all financial institutions.

In contrast, other issues have drawn strong consumer responses that clearly demonstrated consumer interests. For example, the know-your-customer rule proposed by the banking agencies drew over 250,000 public comments, almost all of which objected to the rule on privacy grounds. Similarly, state centralized do-not-call lists have drawn strong responses, with the Indiana Attorney General reporting that nearly one-half of the state's households have opted not to be solicited by telemarketers.

An explanation for the discrepancy between the strong response to the do-not-call lists and the apparent lack of consumer concern over Information Sharing is that the information is consistent. Consumers are not terribly concerned about the Information Sharing by their financial institutions, which, after all, they trust with their actual financial transactions, but consumers respond strongly and in great numbers on other issues that they consider to be covered by the term privacy, including telemarketing and identity theft.

#### **Government Access to Information**

Individuals have long been concerned about government access to information about them. This concern is at the root of the Fourth Amendment limitation on searches and seizures. In the area of consumer financial information, this concern is evidenced by the passage of the Right to Financial Privacy Act of 1978. And, despite the Right to Financial Privacy Act, it was the potential for government access to bank records that spurred much of the public concern over the proposed know-your-customer rule. Concerns over this issue appear to have been reduced by the recognition of the important role that financial institutions can play in the tracking of terrorists that was evidenced by the passage of the USA PATRIOT Act. While Visa believes that consumers will want their financial institutions to continue to work with law enforcement to combat terrorism, there remains a residual concern over unrestricted government access to information when consumers are questioned about "privacy," that is not directly related to the issue of Information Sharing with private parties addressed by the GLB Act.

### **Telemarketing**

While Justice Brandeis is often cited for identifying privacy as the “right to be left alone,” and while certain access to consumer information is necessary in order to engage in telemarketing, consumer concerns about telemarketing are focused more on the intrusive nature of telemarketing calls, and a broad distrust of telemarketers, than on Information Sharing. Although consumers have demonstrated a keen interest in opting out of receiving telemarketing calls in a number of states that have adopted do-not-call registries through their strong responses to those registries, they have not perceived opting out of Information Sharing by their financial institutions as the equivalent.

A far more effective and efficient way to address concerns about telemarketing, and one without the attendant adverse consequences for economic efficiency, would be through appropriately crafted “do-not-call” restrictions. It makes little sense to attack the relatively narrow issue of telemarketing through general restrictions on the disclosure of information where the real issue is the intrusive nature of the telephone calls, and, in some cases, the potential for fraud.

In response to such concerns, the FTC has proposed the creation of a national do-not-call registry. Visa supports a uniform national standard for do-not-call provisions. However, the FTC’s proposal has serious deficiencies because it fails to propose a single uniform national system for addressing the do-not-call issue and it interferes with the ability of financial institutions to serve their existing customers. The fundamental concept of a uniform national do-not-call system should be pursued in order to resolve the telemarketing issue without confusing that issue with Information Sharing.

### **Identity Theft**

Issues relating to identity theft also are often confused with the issue of Information Sharing. Financial institutions recognize that identity theft is a growing problem. In fact, it is a problem for financial institutions as much as it is a problem for consumers. In many situations, financial institutions, particularly in the area of credit and debit card transactions, ultimately bear the financial loss from identity theft. While obtaining a certain amount of information about a consumer is a necessary element in identity theft, there is no evidence that the information that is used to engage in identity theft is obtained through the normal disclosure practices of financial institutions. Pretext calling and other fraudulent or dishonest means are far more likely to be used to perpetrate identity theft than obtaining information from a financial institution by legitimate means. As a result, the issue of the security of consumer financial information and the problem of pretext calling were addressed separately in Title V of the GLB Act.

It also is important to note that the most effective tool in countering the identity thief is information. The ability to perpetrate identity theft involving a financial institution depends on the ability to replicate the information that a financial institution uses to identify prospective customers. To the extent that the financial institution can obtain additional information about an applicant that indicates that the applicant is not who he or she purports to be, or requests information of an applicant where the information provided does not match information verified from other sources, the perpetrator is less likely to be successful in the attempted identity theft. Increasing the information available to financial institutions is more likely to decrease identity theft than to increase identity theft because the identity thief must be able to replicate each piece of information that the financial institution has in order to be confident that he or she can perpetrate the fraud. Accordingly, limiting the information about consumers that is available to financial institutions to verify consumers' identity will inevitably foster identity theft.

Nevertheless, it is appropriate to continue to explore whether additional measures are likely to help prevent identity theft and to mitigate its effects on the victims. In this regard, as financial institutions often bear the brunt of the financial losses associated with identity theft, they have an inherent incentive to prevent identity theft. With this incentive, evolving fraud control systems developed by financial institutions are far more likely to be effective in preventing identity theft than other proposed alternatives, such as mandated requirements to investigate address changes in a particular way or limitations on the disclosures of social security numbers. Indeed, some of these proposals are likely to be counterproductive, with adverse effects far beyond the possible benefits. For example, limitations on the use of social security numbers as identifiers will promote, rather than prevent, identity theft. On the other hand, increased prosecutions and penalties may help serve to deter identity theft.

Even if improved fraud controls and more vigorous prosecutions reduce the frequency of identity theft, they are unlikely to eliminate it entirely. At some point additional fraud controls will not be justified by their costs of implementation. In addition, an unbridled escalation of fraud controls in the credit granting process will make credit more difficult, or at least less convenient, to obtain, as applicants and applications are subjected to extensive additional scrutiny. For example, a simple and well-intentioned requirement to verify an address through a mailing to the consumer before credit is granted would prevent individuals who had recently moved from obtaining point-of-sale retail credit at their new locations.

Accordingly, it is likely that some number of individual victims (albeit hopefully a much smaller number) will continue to suffer the difficulties and inconvenience that result from identity theft. Efforts to correct credit histories and

other records are time consuming, with some reports suggesting that in many cases, hundreds of hours may be involved. Until a satisfactory means can be established to assist these victims, the identity theft issue is likely to continue to draw attention and continue to be confused with the issue of Information Sharing.

### **THE WAY FORWARD**

Legislative solutions to the perceived privacy problem continue to be introduced at both the state and federal level. In order to judge how to respond to these proposals or whether to initiate other proposals, it is necessary to assess the severity of the problem and the appropriateness of the various solutions. Visa has commented on the special issue of affiliate sharing in a separate letter. More broadly, at least with respect to Information Sharing by financial institutions, a strong case can be made that any problems that may have existed have been substantially addressed.

As an initial matter, leaving the issues of government access to information, telemarketing, and identity theft aside, Information Sharing is only of concern to consumers if it is inconsistent with their expectations. Although prior to the GLB Act there were some instances identified where financial institutions may have engaged in Information Sharing practices that were inconsistent with customer expectations, the implementation of the GLB Act privacy rules and the notices distributed by financial institutions to their customers have raised customer awareness of Information Sharing practices, or in economic terms have increased market transparency, sufficiently to conclude that consumers are alerted to the issue of Information Sharing and can make informed choices about the financial institutions with which they wish to deal.

Further, the information derived from GLB Act privacy notices strongly suggests that consumers have a range of choices of financial services providers that do not share nonpublic personal information with third parties outside of the exceptions in the GLB Act. As a result, further legislative mandates on consumer choice, such as an opt-in requirement, are not necessary for consumers who wish to avoid the disclosure of information to nonaffiliated third parties for marketing purposes. For example, notations on a list of over 200 opt-out addresses published on the Web site of the Privacy Rights Clearinghouse indicate that almost 25 percent of the financial institutions listed, including a number of large financial institutions that provide financial services nationwide, do not share nonpublic personal information with nonaffiliated third parties outside of the GLB Act exceptions.

Nevertheless, if further action is deemed necessary, it should be crafted in a manner that best achieves the goal of assuring that customer expectations as to the disclosure of information are met, while minimizing the adverse effects on the efficiencies of Information Sharing. Because efforts to improve market transparency rely on market choices instead of prescriptive rules, efforts to improve transparency



almost always have fewer adverse effects than prescriptive rules. Accordingly, further efforts at improving consumer awareness of Information Sharing practices, or improved transparency, should be explored before prescriptive solutions, such as converting the opt-out right into an opt-in right.

Although there has been much discussion of the complexity of the GLB Act privacy notices, and improvements undoubtedly can be made in this area, there are a number of avenues for improving transparency that may be more effective than focusing on the GLB Act notices. One-on-one disclosures by businesses to customers, such as GLB Act notices, are likely to be inefficient and ineffective where the information to be disclosed is complex, as it is in the case of Information Sharing practices. Because information is already available through the GLB Act notices, private or public secondary sources could evaluate the existing information and provide resources to consumers concerned about privacy, just as the Privacy Rights Clearinghouse has attempted to do.

Further, because the issue of Information Sharing is often confused with issues of government access to information, telemarketing, identity theft, and other issues, a more detailed study of actual Information Sharing practices, similar to the report of The Secretary's Advisory Committee on Automated Personal Data Systems that was prepared within the Department of Health, Education and Welfare in the early 1970s, made readily available and crafted in terms understandable to consumers, would go far to enhance consumer understanding of Information Sharing and would enable consumers to exercise their existing choices about Information Sharing intelligently. Any such report should be coupled with other increased efforts to improve consumer financial literacy. For example, programs such as Visa's Practical Money Skills for Life can improve consumer understanding of the financial system and financial institutions and thereby dispel ungrounded fears about Information Sharing. As Chairman Greenspan testified in a hearing before the Senate Committee on Banking, Housing, and Urban Affairs, "In considering means to improve the financial status of families, education can play a critical role by equipping consumers with the knowledge required to make wise decisions when choosing among the myriad of financial products and providers. This is especially the case for populations that have traditionally been undeserved by our financial system."

Because consumers have a variety of market choices as to how their information may be used, properly informed consumers should be able to make these choices without the need to require individual institutions to tailor their practices to individual consumers. As the Privacy Rights Clearinghouse Survey demonstrates, consumers that object to an individual institution's sharing of information about them with nonaffiliated third parties can vote with their feet.

## RELATED ISSUES

Finally, two related issues also need to be addressed. First, although Congress has addressed the issue of Information Sharing by financial institutions in the GLB Act, much of the current focus on Information Sharing practices focuses on information that is not strictly financial at all, such as information collected on the Internet. To date, Information Sharing is addressed in the United States through a patchwork of laws of which the GLB Act and the rules adopted under the Health Insurance Portability and Accountability Act are perhaps the most comprehensive. In the long run, consistent approaches to Information Sharing are desirable. Even if this goal is not achievable, it is important to ensure that conflicting or overlapping rules do not develop. Not only would such rules increase the costs of delivering privacy protections, but they also would confuse consumers. For example, consumers are unlikely to understand why information collected by financial institutions in person or on paper is treated differently than information collected online, not to mention understanding how information will be treated when it is collected through both sources.

Second, it is important to recognize that financial markets have become national in scope and that individual state initiatives, such as the privacy rules adopted in the state of Vermont last year, have disproportionate effects on national markets, as financial services providers must create exception systems to deal with individual state requirements or modify their entire systems to address the problems created by a single state. In either case, the costs are often borne by consumers outside of the state as well as consumers inside the state.

The need for national uniformity in requirements for use and disclosure of information was recognized by Congress in 1996 in adopting the affiliate sharing preemption provisions in the FCRA. This standard needs to be retained and applied more broadly with respect to Information Sharing by financial institutions. Congress has recognized the importance of financial institutions, and therefore financial information, by adopting comprehensive federal regulatory schemes for the banking and securities industries. Congress also has recognized the trend toward nationwide markets in legislation such as the Riegle-Neal Interstate Banking and Branching Efficiency Act of 1994 ("Riegle-Neal Act"), and more recently the GLB Act and the Electronic Signatures in Global and National Commerce Act ("ESIGN Act"). The adoption of separate state standards for the treatment of consumer financial information would frustrate many of the efficiencies that the Riegle-Neal Act, the GLB Act and ESIGN Act were intended to foster.

Many of the efficiencies from interstate branching and the affiliation of a broader range of financial services companies flow from the ability to centralize data bases and to use information obtained from customers to provide those customers with "one-stop shopping" for financial services. At a minimum, differing state standards for the handling, storage, and use of financial information about customers will lead to the Balkanization of data bases and costly efforts to identify and trace information to ensure that information about a customer that is covered by the law of a particular state is treated in accordance with the laws of that state.

Separate state standards also could require financial institutions to develop and employ different privacy notices and procedures and to apply different standards to the treatment of information relating to a transaction depending on the state where the transaction originated or the state in which the consumer engaging in the transaction resides. In an online transaction where a customer resides in one state, but initiates a transaction to make an investment from the customer's workplace in a second state, and where the financial institution with which the transaction is conducted is located in a third state (as often occurs in the New York City and Washington, D.C. metropolitan areas), as many as three separate state laws could apply to information relating to that transaction. The resulting need to provide multiple disclosures and to apply different standards to the handling of the information would discourage companies from offering the convenience of these services and would only confuse and frustrate consumers. There already is significant concern about the length and complexity of privacy notices that financial institutions must provide to customers, and a proliferation of state privacy requirements will only add to this complexity.

Moreover, the potential consequences of the resulting Balkanization would go beyond individual consumers and businesses to include law enforcement efforts, national security, and the economy as a whole. Consumers will suffer from general confusion and a reduction in the understanding of their rights, greater incidence of identity theft, and higher costs for products and services. Similarly, businesses will suffer through lost efficiencies and increased incidents of fraud. Balkanization of data bases also will make detection of money laundering and tracking of terrorists' activities more difficult for law enforcement, and thereby will adversely affect national security. And, it is important to recognize that the advances in productivity and efficiency that fueled the economic growth of the 1990s are integrally related to uses of information, including consumer financial information, and that further limiting the uses of this information can have immeasurable consequences in terms of innovation and efficiency going forward.

May 10, 2002

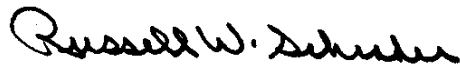
Page 12

As a result, it is essential that any solutions to perceived privacy issues be based on national standards, and meeting those national standards should be sufficient to satisfy any applicable state standards.

\* \* \* \*

Once again, we appreciate the opportunity to comment on this important matter. If you have any questions concerning these comments, or if we may otherwise be of assistance in connection with this matter, please do not hesitate to contact me at (415) 932-2178.

Sincerely,



Russell W. Schrader  
Senior Vice President  
and Assistant General Counsel