30

INDEPENDENT COMMUNITY
BANKERS of AMERICA

May 1, 2002

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

Comments on the GLBA Information Sharing Study

Dear Sir or Madam:

The Independent Community Bankers of America (ICBA)[1] appreciates the opportunity to offer comments for the study being conducted by the Treasury in conjunction with the federal functional regulatory agencies and the Federal Trade Commission on the information sharing practices of financial institutions and their affiliates.

Protection of Customer Information

Community banks have been and will continue to be strong guardians of their customers' privacy and confidentiality. The protection of confidential customer information is central to maintaining public trust and is key to long-term customer retention. Community banks recognize that consumers are concerned about their personal financial privacy, as the technological and electronic revolution transforms financial services operations. At the same time, the ICBA has strongly urged policymakers to maintain an appropriate balance between community banks' legitimate information sharing needs and the critical protection of consumer financial privacy.

The Gramm-Leach-Bliley Act (GLBA) provisions on consumer financial privacy are the most comprehensive, complex privacy protections enacted into federal law. They require banks and other financial services providers to disclose their privacy

[1] ICBA is the primary voice for the nation's community banks, representing 5,000 institutions at more than 17,000 locations nationwide. Community banks are independently owned and operated and are characterized by attention to customer service, lower fees and small business, agricultural and consumer lending. ICBA's members hold more than $511 billion in insured deposits, $624 billion in assets and more than $391 billion in loans for consumers, small businesses and farms. They employ nearly 231,000 citizens in the communities they serve.

policies and practices to customers annually, and give customers an opportunity to "opt-out" before nonpublic personal information is disclosed to nonaffiliated third parties. The legislation includes a number of critical exceptions that permit information sharing with third parties for legitimate purposes such as outsourcing, joint agreements to provide financial products and services, and routine processing and servicing of accounts and transactions.

Various state legislatures have considered financial privacy legislation that would impose different requirements and restrictions than GLBA. The ICBA believes that the GLBA – which was fully implemented in July 2001 – should be allowed to work and the effects and consequences of GLBA properly assessed before additional legislation is enacted in the financial privacy area. The ICBA also supports federal preemption of state law in this area to prevent a patchwork of state laws with divergent privacy protections.

Following are the ICBA's comments to some of the specific questions raised by the Treasury in the *Federal Register*. As requested, we have indicated to which specific questions our comments apply, although we have combined some responses to better address the issues presented.

Information Sharing by Community Banks

Questions 1 (a) through (e)

Community banks generally restrict information sharing to instances where it is necessary to process transactions or to provide financial services to customers. However, where a community bank shares customer information to process a transaction or to provide a product or service, it often relies on trusted third party processors and vendors. These arrangements allow community banks and their customers access to more efficient data processing services, to provide and process checks, and to provide products and services such as credit cards, mortgages, insurance and securities transactions. When information is shared, it is generally restricted to other banks, check printers, credit bureaus and other service providers and to the information necessary to provide the process, product or service.

Community banks operate under a different corporate structure than do many large complex banking organizations. Larger corporations have within the holding company umbrella many different companies. In part, the structure of a large organization may be the result of differing state laws and regulations, historical acquisitions, and tax ramifications. However, it is important that policymakers recognize that larger companies can offer a wide variety of financial services within the corporate family. The Gramm-Leach-Bliley Act recognized this clearly by creating a new entity, the financial holding company, which can offer banking, securities and insurance services under one corporate umbrella. For these large companies, information sharing with affiliates becomes the key to serving customers. Community banks, on the other

hand, must turn outside to provide a competitive alternative for many of the same products and services and thus rely more heavily on non affiliates.

Even large complex banking organizations, though, rely from time-to-time on outside service providers to meet customer needs. For community banks, which operate with a much simpler corporate structure, the use of outside service providers and partners is critical. These non-affiliates allow community banks to provide the same types of products and services that much larger banks can and do. For many community banks, partnering with these trusted third parties is the only way the bank can offer the services to its customers.

In addition, banks of all sizes rely on third parties to meet a variety of needs, from data processing to check printing and for other administrative purposes. In many instances, third parties can provide these functions more efficiently and less expensively than the bank could for itself. And, to take advantage of these third party service providers, banks must share a certain amount of customer information.

The Gramm-Leach-Bliley Act, by allowing financial holding companies to provide a variety of financial services under one corporate umbrella, recognizes the increasing importance being placed on access to a variety of financial products and services through one trusted provider. Because they do not have an extensive array of affiliates within the corporate structure to provide different products and services, allowing community banks to share information with non-affiliated service providers and joint marketers permits community banks to offer a breadth of financial products and services to their customers at a reasonable cost, something they might not otherwise be able to offer. For customers of community banks in rural areas, where the number of financial service providers may be limited, this gives individuals access to financial products and services that might otherwise not be readily available from a local provider.

When any bank, large or small, enters an agreement with a service provider or joint marketer to provide a product or service for its customers, it only does so after carefully considering the performance record of the other company. Community banks do not want to jeopardize their reputations with customers by contracting with a third party provider or joint marketer that will have a negative impact on the bank's customers. When establishing these arrangements, community banks ensure that their partners will maintain appropriate confidentiality. Indeed, under the provisions of the Gramm-Leach-Bliley Act, banks must incorporate requirements of confidentiality of customer information in their contractual arrangements with third parties. However, as noted above, when they do share information, community banks generally restrict it to that information needed by the service provider to perform the service for which the bank has contracted.

The Gramm-Leach-Bliley Act recognized the importance of information sharing by creating a series of exceptions to the general restriction on sharing information without notice and an opportunity to opt out. Much of the information sharing by

community banks is covered by one of these exceptions. These exceptions, therefore, are vitally important to permit community banks to serve their customers.

Question 1(h) For what other purposes would financial institutions like to share information but currently do not?

The ICBA is not aware of any purposes beyond those currently permitted. However, it is also important to recognize that as technology and the economy change, any restriction on information sharing adopted in today's environment may negatively affect the ability of financial institutions to serve their customers in the future. Therefore, it is very important to allow sufficient flexibility for banks and other financial institutions to adapt to changing demands and environment.

Security Protections

Questions 2 (a) and (b)

Community banks value customer information, and take appropriate steps to safeguard the security of that information. Employees are trained against sharing information inappropriately, and community banks use procedural, physical and electronic measures as appropriate to restrict access to customer information. The use of passwords to access databases and regular training sessions for employees are among the tools community banks use to safeguard customer information.

In February, 2001, as required by the Gramm-Leach-Bliley Act, the Federal Financial Institutions Examination Council (FFIEC) issued guidelines for safeguarding customer information that all banks and savings associations must follow. Under these guidelines, banks and savings associations must establish comprehensive, written security programs that include administrative, technical and physical safeguards appropriate to the institution's size and the complexity and scope of their activities. These programs are designed to ensure the confidentiality and security of customer information; protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. Under these guidelines, banks must continually train employees, audit for compliance and regularly review their information security programs. Although banks had taken many of these steps before the guidelines became effective, these new guidelines ensure that every bank and savings association will carefully analyze its existing information security program and, where necessary, update it. In addition, the events of September 11 have made many banks even more sensitive to the needs to ensure that appropriate safeguards are in place to protect customer information.

Therefore, the ICBA believes that existing statutory and regulatory requirements are adequate to protect customer information.

In a recent issue of its *Suspicious Activity Report Review,* FinCEN identified identity theft as a critical and growing problem for consumers. This growing problem has focused new attention on the security of customer information. However, it is important to recognize also that not all information about consumers -- in fact, not even all financial information about consumers – is housed in banks and banking organizations. Consumers themselves often provide information for a variety of reasons, such as when making a purchase or even entering a contest on the Internet. And, public records also make some consumer financial information readily available, such as information in real estate records. While banks take many steps to protect customer information, customers themselves also bear a certain responsibility to protect their own information.

Potential Risks and Benefits from Information Sharing

Questions 3, 4 and 5

Banks and, more importantly their customers, benefit from information sharing by providing access to products and services that might not otherwise be possible. For smaller community banks with limited resources, this allows them to provide a level of customer service and satisfaction that might not otherwise be possible. For example, small community banks may not have the internal resources to manage a credit card operation, but by entering into a joint venture with a credit card issuer, the bank is able to offer its customers credit cards. As another example, entering into arrangements with securities brokerages allows smaller banks to offer their customers securities services. Without information sharing, smaller banks might not find it economical or convenient to offer these types of services. And as noted above, if the local bank were unable to provide them, it would mean that consumers in some rural communities would not have local access to these products and services.

Customers also benefit from information sharing by targeted information about new products and services. And as technologies become more sophisticated, banks will be able to even better tailor information about products or services for a specific individual.

For example, access to credit is increasingly important. Accurate reporting through credit bureaus allows lenders to properly assess and compete for consumer loans. The increased competition for consumer lending gives individual consumers access to a broader variety of loan products at lower prices. Without the information sharing through credit bureaus, this competition and access to credit would be substantially diminished.

Information sharing also provides both banks and the federal government with tools to inhibit money laundering and terrorist activities. In fact, under the recently enacted USA-PATRIOT Act, the Department of the Treasury is under a mandate to take steps to facilitate information sharing about these activities among banks and between banks and law enforcement. This kind of information sharing helps banks to detect

fraud and deter criminal activity, especially money laundering. While it is important that an appropriate balance be struck between privacy and information sharing, information sharing is clearly important to prevent fraud, money laundering and terrorist activities.

Further limits on access to information would also make it more difficult for banks, especially community banks, to serve their customers. Second, it would increase the costs of providing products and services to customers. Third, it would restrict the variety of financial products and services community banks can offer their customers, since many products and services that cannot be offered as efficiently or cost effectively in-house are currently offered through third party service providers and joint marketers.

Ready access to customer information does carry certain risks, however. The more places that information can be accessed, the greater the risk. For that reason, community banks take appropriate steps to safeguard customer information in accordance with existing regulations and the long-standing policies and practices.

Identity theft is one such risk. To help prevent identity theft, banks have undertaken a variety of educational steps to help customers protect their own information as it is increasingly important that customers share in security responsibility. For example, it is critical that consumers promptly reconcile bank statements, destroy credit card receipts when no longer needed, and properly dispose of financial statements and financial records so that information cannot easily be stolen from trash receptacles. Similarly, customers should not give out information about their accounts or financial activities without knowing to whom they are providing that information. Banks and federal regulators can help educate customers about these practices.

Adequacy of Existing Laws to Protect Customer Privacy

Question 6 (a) and (b)

The ICBA believes that existing laws, such as the GLBA privacy requirements and the Fair Credit Reporting Act, adequately protect the security and confidentiality of customer information. There are also a variety of other federal requirements, such as the Electronic Fund Transfer Act and the Truth-in-Lending Act, and their implementing regulations, that provide mechanisms that help to protect customer information.

Unlike the Fair Credit Reporting Act, though, which included a temporary pre-emption of state law, the Gramm-Leach-Bliley Act almost encouraged states to adopt differing standards for customer information. It is very important that the federal government adopt and implement a uniform standard for information sharing to avoid a patchwork of varying state requirements. A varied set of information sharing requirements can be detrimental for banks and their customers.

Already, some states have instituted or are considering differing standards for information sharing. For example, California is considering legislation that would

require customers to "opt-in" before much information could be shared. One estimate suggests that this could cost California users of credit cards as much as $927 million more each year, and that the average California home purchaser would pay $1,760 more in interest on a new home.[2]

Many banking organizations, even smaller community banks, offer products and services to customers in more than one state. Requiring banks to comply with a variety of differing privacy standards only serves to increase compliance costs. In other instances, banks may decide that it is easiest not to offer their products and services to customers in other states to avoid these compliance hurdles. For example, Vermont recently adopted rules that require an "opt-in" for Vermont customers. As a result, residents of Vermont may not have access or information about a broad variety of products and services because banks will treat all Vermont residents as having opted out, thereby restricting their access to a variety of different products and services.

Beside increasing compliance costs, differing state laws and standards will also engender customer confusion. Having a national standard for customer information sharing would avoid the confusion and costs that result from a variety of differing state requirements.

Privacy Notices. Since the first round of privacy notices required by the Gramm-Leach-Bliley Act were delivered last summer, there has been much discussion about the adequacy of those notices and whether a simpler format would be useful. Unfortunately, the specifications in both the law and the privacy regulations prevented financial institutions from offering a simple notice to their customers. The ICBA believes that a simpler, more straightforward notice would be useful, but to do so would require Congressional action.

Many community banks are not required to offer their customers an opt out, because the information that is shared, if any, is covered by one of the exceptions under the Gramm-Leach-Bliley Act. Unfortunately, the media focused on the importance of exercising the right to opt out. As a result, some community banks that did not offer an opt-out received requests from customers to opt out. It is important, then, that federal authorities help banks educate the public about the law and its requirements to correct the misperception fostered by the media.

In addition, for many community banks that do not share information outside one of the exceptions, the initial notice provided to customers was more limited in scope. Unfortunately, current regulations require that the notice be provided annually, at a substantial cost, a cost that will increase when postage rates increase this summer. Rather than requiring an annual privacy notice, if the privacy policies and procedures of a bank have not changed, it would be simpler and more cost effective – and less confusing to customers – to provide the privacy notice at account opening and then

---

[2] *The Hidden Cost of Privacy: The Potential Impact of 'Opt-in' Data Privacy Laws in California*, study by the Direct Marketing Association, 2002.

again only if and when the privacy notice changes. This would also call to a customer's attention the fact that there has been a change to the policy.

Different Approaches

Questions 8 and 9

The ICBA questions whether opt-in would be a feasible approach for governing the sharing of customer information. As noted above, the costs to consumers in California suggest that an opt-in approach is not beneficial to either consumers or banks. And, if opt-in was applicable to any of the existing exceptions under GLBA, it would have a substantial negative impact on the ability of community banks to serve their customers.

Finally, the ICBA believes that before any additional restrictions are placed on information sharing by banks, it is critical that customers understand the impact that those restrictions could have on how they conduct their financial affairs. For example, many customers might be willing to opt against having information shared with a credit bureau, until they became aware of the impact it had on their access to credit services. It is important that the terms privacy and information sharing be better defined and understood by the general public before additional restrictions are contemplated.

If you need any additional information or wish to discuss any of the points covered in our letter further, please contact Rob Rowe, ICBA's regulatory counsel, at 202-659-8111 or by e-mail at robert_rowe@icba.org.

Thank you for the opportunity to comment.

Sincerely,

A. Pierce Stone
Chairman