

900 Nineteenth St. NW, Ste. 400  
Washington, DC 20006  
TEL: (202) 857-3100  
FAX: (202) 296-8716  
E-MAIL: info@acbankers.org  
http://www.AmericasCommunityBankers.com



May 2, 2002

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

Re: Study on Information Sharing Practices Among Financial Institutions and Their Affiliates  
67 FR 7213 (February 15, 2002)

Dear Madam or Sir:

America's Community Bankers ("ACB")<sup>1</sup> welcomes the opportunity to provide comment to the Secretary of the Treasury and the federal financial regulatory agencies (the "agencies") on their study of the information sharing practices (the "study")<sup>2</sup> among financial institutions and their affiliates required by the Gramm-Leach-Bliley Act of 1999 ("GLBA")<sup>3</sup>. Treasury and the agencies have requested specific comment on the purposes, benefits, and costs associated with the sharing of customer's nonpublic personal information by financial institutions with corporate affiliates or non-affiliated third parties.

**ACB Position**

In protecting customer information, community banks adhere to responsible information sharing practices and take extraordinary precautions to protect customer information. As described in detail throughout this letter, community banks primarily share customer information on a very limited basis to conduct transactions, protect against fraud, improve customer support, and to market their own products to their customers. These institutions all have in place policies, procedures, and systems dedicated to protecting customer information. ACB believes that the GLBA information security requirements create an effective framework for protecting nonpublic personal information, and that more time is needed to evaluate whether additional protections are needed that may unduly burden community banks without providing any additional protections.

<sup>1</sup> ACB represents the nation's community banks of all charter types and sizes. ACB members, whose aggregate assets exceed \$1 trillion, pursue progressive, entrepreneurial and service-oriented strategies in providing financial services to benefit their customers and communities.

<sup>2</sup> 67 Fed. Reg. 7213 (Feb 15, 2002).

<sup>3</sup> Pub. L. 106-102, Title V, Sec. 508.

## Background

Pursuant to the GLBA, the Secretary of the Treasury, in consultation with the agencies, is required to study and report back to Congress on the information sharing practices of financial institutions. The study is to focus on the manner in which financial institutions share confidential consumer information with corporate affiliates and non-affiliated third party organizations. Treasury's report to Congress is to include findings of the study, along with recommendations for any needed legislative or administrative action.

In order to conduct the study, Treasury issued a request for comment on February 15, 2002<sup>4</sup> that posed forty-five questions relating to a broad range of information sharing issues. The questions covered issues such as: purposes of information sharing; costs/benefits associated with information sharing; adequacy of existing laws/regulations; tactics for protecting customer information; feasibility of requiring affirmative customer response prior to information sharing (opt-in); and others.

## General

There are several existing laws that restrict how financial institutions use and share customer information. Perhaps most significant are the privacy provisions of the GLBA<sup>5</sup>, which represent the most comprehensive privacy protections, yet enacted into federal law. The regulations issued pursuant to the GLBA require all financial institutions to: (1) create a notice that accurately reflects its policies and practices; (2) provide a privacy notice to customers at the initiation of the relationship and annually thereafter; (3) generally refrain from sharing nonpublic consumer information with nonaffiliated third parties, unless the consumer is provided the opportunity to prevent such sharing (opt-out); and (4) refrain from sharing customer account numbers that could be used in conjunction with marketing activities.

In addition to the privacy provisions found in the GLBA, community banks are subject to a number of other existing statutes and regulations. The Fair Credit Reporting Act<sup>6</sup>; the Expedited Funds Availability Act, and its implementing regulation—Regulation E<sup>7</sup>; and the Right to Financial Privacy Act<sup>8</sup> are examples of federal law designed to protect consumer privacy and restrict unnecessary information sharing. These legal and regulatory requirements attempt to satisfy the delicate balance of protecting consumers, while preserving the flexibility necessary to conduct financial transactions. When considering recommendations for future legislative or administrative action, ACB urges Treasury and the agencies to take into account the outstanding record community banks have in protecting consumer financial information, and the need to strike the appropriate balance between legitimate information sharing practices and protecting consumer financial information.

---

<sup>4</sup> 67 Fed. Reg. 7213 (Feb. 15, 2002).

<sup>5</sup> Pub. L. 106-102, Title V.

<sup>6</sup> 15 U.S.C. § 1681.

<sup>7</sup> 15 U.S.C. § 1693.

<sup>8</sup> 12 U.S.C. § 3401-3422.

## **Overview of Community Bank Information Sharing Practices**

Protecting and safeguarding customer information is the cornerstone of every community bank's relationship with its customers. Few responsibilities of managing a modern community bank are considered more important, or taken more seriously. Community banks primarily share customer information to conduct transactions, ensure accurate consumer reporting, inform customers of new opportunities, and combat fraud. And when sharing customer information is required, community banks consistently practice responsible information sharing practices. The information sharing activities of community banks can result in tremendous benefits for consumers, such as reducing exposure to fraud, providing access to new financial products and offering improved customer service.

Community banks also share information in ways that help ensure funding is available to help families achieve the dream of homeownership. By participating in the secondary mortgage market, community banks have access to an important source of capital that enables them to provide affordable home loans to consumers. Without such information sharing necessary for secondary mortgage transactions, consumers would be faced with increased lending costs that could price some families out of homeownership.

### **Information Sharing Benefits**

The responsible sharing of customer information with affiliates and non-affiliated business partners can be the source of a wide range of benefits to consumers and community banks. It is also important to observe that often financial services affiliations are transparent to consumers. What may appear to be a single financial institution offering traditional financial products, insurance and brokerage services, may represent three different business entities operating under one corporate umbrella. And while most information sharing conducted by community banks is done primarily to facilitate transactions, other forms of information sharing provide direct benefits to both consumers and community banks. These include:

- *Assessing Consumer Needs* – By assessing consumer needs, community banks are able to better align the needs of consumers with products/services offered. Providing consumers with products/services at a competitive price and strengthening customer relationships.
- *One-Stop Call Centers* – In order to remain competitive in today's marketplace, some community banks are establishing insurance and brokerage businesses; or partnering with others to complement their traditional financial product lines with a single service center for all products. Information sharing is critical to provide customers with a convenient way to obtain customer support on a full suite of financial products.
- *Fraud Prevention* – By sharing information about customer transactions, institutions are able to identify potentially fraudulent transactions that can reduce the costs and burdens to both customers and financial institutions.

- *Online Product Offerings* – For institutions offering a range of products and services through affiliates and business partners, the Internet provides a great medium to provide cost-effective and centralized access to consumers' accounts. Information sharing makes these services possible.
- *Consolidated Billing Statements/Operations Centers* – Diversified financial institutions can now provide customers with information on all of their accounts (e.g., savings, investment, etc.) in a single statement. This allows consumers to obtain a more complete picture of their financial status and better manage their finances. Using centralized operations centers to process and print statements can generate savings, which can be eventually passed down to consumers.
- *Minimizing Mass Marketing Techniques/Costs* – Responsible information sharing provides valuable data for developing marketing campaigns that help minimize the deluge of brochures, statement stuffers, and other marketing confronting consumers every day. This also helps financial institutions control costs and direct products and services to consumers who are most likely to be interested in them.
- *Providing Quick Access to Products/Services* – An increased use of technology and responsible information sharing practices has enabled consumers to obtain credit and loan approvals in minutes, as opposed to days and weeks. Without the ability to share information with credit reporting agencies, business affiliates, and others, approval times would be lengthened and consumers could be forced to pay higher rates, as institutions are unable to efficiently evaluate individual credit risk.

In summary, responsible information sharing practices allow community banks to facilitate transactions, protect their customers, understand customers' financial needs, and improve overall customer service. The benefits from responsible information sharing can result in significant economic benefit for both consumers and financial institutions. Additional restrictions on information sharing could produce unintended consequences that could negatively affect all types of financial institutions and the overall economy.

### **Protecting Customer Information**

Protecting confidential customer information within community banks has long been an institutionalized part of the culture of bank management. Consideration goes beyond simply protecting information within the walls of the institution, it includes protecting information shared with affiliates and non-affiliated third parties alike. The majority of community banks have in place specific programs focused directly on protecting customer information. These include board approved strategies and policies; training and awareness programs; and an assortment of technology solutions.

In addition, pursuant to the GLBA,<sup>9</sup> as of July 1, 2001, all financial institutions must perform an assessment to identify the risks that threaten the security, confidentiality, or integrity of customer

---

<sup>9</sup> Pub. L. 106-102, Title V, Sec. 508.

information. Each institution is required to develop a written information security program that properly reflects the size and complexity of the institution, as well as the nature and scope of its activities. These information security programs must be board approved and reflect that specific safeguards are considered, including encryption of customer information, access control restrictions, intrusion detection monitoring, and appropriate procedures for security breaches. In addition, the regulations issued pursuant to the GLBA require all financial institutions to take steps to oversee service provider arrangements<sup>10</sup> where customer information may be shared with non-affiliated third parties. Under GLBA, all financial institutions must have contractual provisions that require service providers to have programs to ensure the security and confidentiality of customer information.

The long history of financial institutions' efforts to protect customer information, along with the GLBA information security program requirements help create the framework of an effective defense system to protect customer information. Moreover, the GLBA information security program requirements have existed for less than ten months. ACB believes that existing legal and regulatory requirements adequately protect customer information at this time, and that more time is required to evaluate the effectiveness of these requirements before additional requirements on the industry are considered.

### **Protecting Against Fraud**

One area that ACB believes Treasury's study should pay particularly close attention to is the way in which community banks—and others—share and utilize information to combat fraud. By all accounts crimes related to identity theft are increasing dramatically, and one of the ways community banks are able to facilitate the detection of identity theft and protect against other types of fraud is through the use of various fraud detection programs. These programs operate in a secure environment where information on individuals may be obtained by a bank prior to opening an account or conducting a transaction. These systems are a key tool in identifying individuals suspected of being involved in some type of fraud scheme, and protecting a consumer who has been a recent victim of identity theft.

Information sharing in these programs is tightly controlled and a "positive hit" on one of these systems would not necessarily prevent an individual from conducting a transaction, rather it would result in increased due diligence on the part of the bank. These programs help protect consumers, and are a key risk management tool for banks of all sizes.

### **Opt Out vs. Opt In Approaches to Customer Consent**

Under the current legal and regulatory framework, consumers must be provided the opportunity to direct financial institutions to refrain from sharing nonpublic personal information with nonaffiliated third parties (GLBA), and to refrain from sharing credit report related information with affiliates (FCRA). This "opt out" approach has proven to be an effective way for

---

<sup>10</sup> The final rule, as jointly approved by the agencies, has four separate citations: 12 CFR Part 30 (OCC); 12 CFR Parts 208, 211, 225, and 265 (Federal Reserve); 12 CFR Parts 308 and 364 (FDIC); and 12 CFR Parts 568 and 570 (OTS).

consumers to exercise their information sharing preferences, and represents the least burdensome alternative for community banks. This helps reduce costs to institutions, which in turn can be passed on to consumers in the form of lower fees and more competitive lending rates.

Compliance costs for institutions offering opt-out are significantly higher than for those that choose not to share customer information outside the limited exceptions provided under current law. This is due in part to system requirements and increased demand for support personnel needed to process consumer requests. For those institutions that choose to share customer information, offering customers access to diversified products and services that the typical community bank may not otherwise have the capability to offer can offset these costs. For community banks, the benefit goes well beyond the nominal fee revenue such arrangements generate, rather it can help community banks remain competitive with large mega-banks that are able to offer a wide-range of products within a corporate family of affiliated companies.

Some policymakers at the state and federal level are advocating information sharing restrictions based on an "opt in" methodology whereby institutions would be required to seek the affirmative consent of all customers to each institution's privacy policies. This approach could have the unintended consequences of restricting information sharing that could eliminate some or all of the aforementioned benefits to consumers, and result in significant financial loss to banks both in terms of lost opportunities and potential fraud exposure. As discussed below, the overwhelming evidence to date indicates that most customers are comfortable with their institutions' information sharing practices. The prospects of having to comply with federal and state specific privacy methodologies creates an administrative nightmare for all financial institutions to obtain customer's information sharing preferences without any clear incentive for doing so.

### **Customer Reaction to Information Sharing Restrictions**

In a recent survey, ACB asked community banks to gauge customers' reaction to privacy policies and estimate the costs for complying with the GLBA privacy provisions<sup>11</sup>. ACB found that most institutions surveyed received little, or no feedback from customers regarding privacy policies. Of those institutions reporting some customer feedback, almost half (43 percent) found the privacy disclosures somewhat or very useful. Perhaps most significant in the survey was the relatively few number of customers who, when given the choice, requested their bank refrain from sharing information with nonaffiliated third parties. While ACB found that most community banks do not share customer information with non-affiliated third parties—beyond the basic exceptions provided under GLBA—those few who are subject to the GLBA opt out indicate that the overwhelming majority of customers choose not to exercise this right. ACB believes that the fact so few customers elected to exercise their opt out right indicates the level of trust placed in the ability of community banks to protect customer information.

### **Information Sharing with Affiliates vs. Non-Affiliated Third Parties**

Recognizing that greater control and protection of customer information exists when it is confined within a single corporate family, current laws and regulations distinguish between

---

<sup>11</sup> *ACB Privacy Compliance Survey*, America's Community Bankers, December 3, 2001.

information sharing conducted with affiliates and non-affiliated third parties. As a result, financial institutions face fewer restrictions when sharing information with affiliates, than when sharing with non-affiliated third parties. Moreover, the benefits of information sharing within a corporate family were recognized by Congress during the consideration of GLBA, where throughout the legislative process amendments to impose opt-out requirements on affiliate information sharing were explicitly rejected. Pursuant to the GLBA, information-sharing restrictions are directed at the exchange of information with non-affiliated third parties only. ACB believes this is appropriate, since greater control over how customer information is used and disseminated exists within a corporate family.

More community banks are establishing business relationships with non-affiliated third parties to offer a wider-range of products and services to compete with large mega-banks that are able to offer many different products within a corporate family of affiliated companies. Its important to note that community banks do not share nonpublic personal information with non-affiliated third parties without making certain that customer information will be properly protected. This is done not only as a regulatory requirement, but as a common-sense business practice intended to protect customers and minimize potential reputation risk. For example, when entering into agreements to offer credit cards to customers, community banks often impose significant restrictions on marketing and customer contact (e.g., no telemarketing calls, limit two mailings/year, etc.). These types of contractual restrictions are in addition to the GLBA requirements for ensuring that business partners effectively protect nonpublic personal information. When considering information restrictions on non-affiliated third parties, policymakers need to balance consumer privacy concerns, with the need for community banks to utilize business partnerships to offer their customers a diverse set of financial products and services that empower them to compete with large mega-banks.

#### **Suggested Statutory or Regulatory Changes**

In seeking public feedback on the information sharing practices of financial institutions, Treasury specifically requested comment on the adequacy of existing privacy laws and regulations, and what new or revised laws and regulations may be necessary. ACB believes that the existing framework of privacy protections and disclosure requirements (e.g., GLBA, Right to Financial Privacy Act, FCRA, Reg. E, etc.) adequately protect customer information and communicate to consumers how information is used. Enacting new restrictions or placing additional requirements on financial institutions is unnecessary at this time.

The privacy provisions of the GLBA have been in place now for less than one year, and more time is needed to assess their effectiveness. While ACB believes more time is needed to assess the GLBA privacy provisions, there may be specific legislative and/or regulatory changes that could be considered that would reduce consumer confusion and minimize burdens placed on financial institutions.

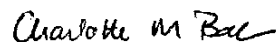
In particular, it may be appropriate for the study to consider whether reducing the disclosure burden on community banks that conduct only limited information sharing practices may be appropriate. Pursuant to the GLBA, financial institutions must provide customers with an annual privacy policy notice. This is a costly burden and annual expense for community banks.

Moreover, because the overwhelming majority of community banks are not subject to the opt-out requirement, there is no need to obtain customer response and subsequent annual notices will most likely repeat what has already been disclosed. ACB suggests that the study consider the value of annual notices, especially for those institutions that: (1) have not changed their notice since it was last provided to the customer; (2) refrain from sharing customer information outside the limited exceptions in the law; and (3) are not subject to the opt-out requirement. ACB believes that both financial institutions and consumers would be better served if the disclosure requirements for institutions not subject to the opt-out were simplified, with subsequent notices required only when an institution's privacy policy is revised. This would minimize the number of disclosures customers receive—increasing the likelihood that they would actually be read—and minimize the burden placed on community banks.

### **Conclusion**

Thank you for the opportunity to comment on this important study. ACB stands ready to work with Treasury in any way possible to help provide some perspective on the information sharing practices of community banks. Should you have any questions, please contact the undersigned at 202-857-3121 or via email at [cbahin@acbankers.org](mailto:cbahin@acbankers.org); or Rob Drozdowski at 202-857-3148 or via email at [rdrozdowski@acbankers.org](mailto:rdrozdowski@acbankers.org).

Sincerely,



Charlotte M. Bahin  
Director of Regulatory Affairs  
Senior Regulatory Counsel