36

May 1, 2002

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

Attention: Study on GLBA Information Sharing

Re: ***Comments on the GLBA Information Sharing Study***

Dear Sir or Madam:

The Connecticut Bankers Association ("CBA" or "Association") is pleased to submit the following comments to assist the Department of the Treasury in its study on the information sharing practices of financial institutions.

By way of background, the Connecticut Bankers Association is an industry trade association that represents over eighty (80) banks and thrifts conducting banking operations in the state of Connecticut. Association membership is comprised of a wide variety of different types of institutions. The field of membership ranges from small community banks all the way to large, multi-state institutions. Although the CBA does not purport to speak for every member institution, the comments set forth below have been formulated on the basis of comments the CBA has received from its member institutions. Naturally, some of our members could have different views.

As additional background, you should note that within the CBA membership there are different organizational and product-delivery structures. For example, a number of member banking institutions do not have any "affiliates". Others have subsidiaries or other affiliates that perform functions that the bank could perform itself (e.g., subsidiaries to service mortgage loans or to hold foreclosed real property). Some members have affiliates that provide certain nontraditional services to bank customers (e.g., a broker-dealer subsidiary or an insurance agency subsidiary). Other member banks provide nontraditional products and services to their customers through *contractual* networking arrangements with *nonaffiliated* third-party financial institutions (such as a third-party broker-dealer or insurance agency). These networking arrangements are most prevalent with the smaller community banks that are not large enough to provide these services through a wholly-owned subsidiary (or some other "affiliate" relationship).

In this letter, we will attempt to provide comments that are relevant to each of these different structural perspectives. However, once again, we cannot purport that the expressed views are shared by all members within a particular structural class.

Set forth below are answers to some of the questions you have posed in your request for comments. For convenient reference, we have repeated the applicable questions (and included the corresponding number and letter from your request).

1. Purposes for the Sharing of Confidential Customer Information with Affiliates or with Nonaffiliated Third Parties.

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

Subject to certain important exceptions, banks share many different "types" of information with their affiliates. That information could include "experience or transaction" information, such as deposit balances or payment history. It could also include certain nonexperience information, such as credit reports or information contained in applications.

This is not to suggest that every type of information is likely to be shared between a bank and its affiliates. In most cases, banks have policies in place that are designed to ensure that information is not shared without an appropriate *purpose* being present (see section 1d below). This general prohibition helps to ensure that access to nonpublic personal information is limited to persons within the corporate family who have a need to know. In addition, in some cases, the sensitive nature of certain information might be such that an institution has a policy which prohibits, altogether, the sharing of that type of information (e.g., medical information).[1] There may also be certain legal reasons why certain types of information are not shared (e.g., the consumer has opted out under the FCRA with respect to nonexperience and nontransaction information).

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

As a "general" rule, banks are more restrictive in their information sharing practices when it comes to *nonaffiliated* third parties. This attitude generally reflects the notion that consumer privacy expectations are often elevated in the "nonaffiliate" context.[2] For these reasons, fewer "types" of information are shared among nonaffiliated third parties.[3]

---

[1] Naturally, there may be instances where sensitive information (such as medical information) will be shared because the exchange of information is required to conduct operations (e.g., in connection with the sale of credit life insurance).

[2] We note that many of the smaller institutions use nonaffiliated third parties to perform services and functions that are typically performed by "affiliates" for some of the larger financial institutions. In these cases, the types of information are similar to those discussed in section 1a above.

[3] We also note that both state and federal privacy laws restrict certain "types" of information from being shared with nonaffiliated third parties. For example, because of concerns under the FCRA, it is less likely that "consumer

Nevertheless, there are still many different types of information that might be shared with nonaffiliated third parties. Although it is difficult to provide a comprehensive list, the information can include just about any type of experience or nonexperience information where the disclosure is necessary to conduct business operations or comply with the law.

c. Do financial institutions share different "*types*" of information with affiliates than with nonaffiliated third parties? If so, please explain the differences in the types of information shared with affiliates and with nonaffiliated third parties.

As is discussed above, there are differences in the *types* of information shared with affiliates and with nonaffiliated third parties. For example, because of *state statutory* restrictions, banks operating in Connecticut are typically prevented from sharing *deposit* information with a *nonaffiliated* third party. In contrast, because of a federal preemption provision (i.e., contained in the FCRA), that state statutory restriction does not operate to restrict the sharing of *deposit* information among *affiliated* entities. As a result, many of the larger institutions share deposit information among affiliates (e.g., to help an affiliated broker-dealer better identify and/or anticipate customer needs), whereas state law would prevent that same "type" of information (i.e., deposit information) from being shared with a nonaffiliated third party (i.e., with a broker-dealer in a contractual third party networking program). Note that this state law preemption anomaly presents a competitive disadvantage for smaller community banks (see the discussion in section 6a below).

There are other differences that are driven by federal law concerns. For example, affiliated institutions can (and sometimes do) share *nonexperience* and *nontransaction* information (e.g., credit reports), subject, of course, to the FCRA opt-out rules. In contrast, subject to certain exceptions, nonaffiliated third parties are unable to share that type of information without being subject to the burdensome rules that are applicable to consumer reporting agencies under the FCRA. Again, this anomaly presents certain competitive disadvantages for smaller community banks (see the discussion in section 6a below).

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

There are many different types of *purposes* for sharing information with *affiliates*. In many cases, affiliates perform functions that the bank could perform itself. For example, it is common in Connecticut for a bank to own a subsidiary that holds and services mortgage loans that have been originated by the parent-bank. Within the parent-subsidiary family, it is not uncommon for the entities to exchange information in order (i) to better serve the customers, (ii) to enhance operational efficiencies, or (iii) to achieve certain safety and soundness objectives.

---

report" information would be shared with nonaffiliated third parties (except for permissible purposes). By way of additional example, Connecticut has a state law restriction on the sharing of certain deposit information (see the discussion in section 6a of this letter).

For example, if a customer notifies the bank of a change-of-address, that information might be shared throughout the corporate family for the purpose of making sure that all mailing addresses are current (e.g., for deposit accounts at the bank level and mortgage relationships at the subsidiary level). It is a matter of good *customer service to* establish systems that eliminate the need for a customer to have to submit multiple requests for a change of address.

As for purposes related to *operational efficiencies*, affiliated institutions will often share information in order to save time and money for the customer and/or the financial institution. For example, subject to certain legal conditions (e.g., FCRA opt-out rights, among others), affiliated entities may want to share a recent credit report or appraisal when a consumer applies for a new mortgage loan product within the corporate family. This practice can save the applicant both time (i.e., waiting for an appraisal) and money (i.e., paying for a new credit report or appraisal).

As for purposes related to *safety and soundness*, affiliated entities might, for example, share information that would help an institution better underwrite a credit application (e.g., experience, transaction, or other information) or to help with collection efforts (e.g., location of debtor or debtor's assets). Enhanced safety and soundness ultimately leads to lower cost products and services for consumers.

In addition, affiliated entities sometimes share information for *marketing* purposes. However, before engaging in a particular information-sharing practice for marketing purposes, the institution will typically try to weigh customer expectations and potential consumer benefits. For example, to the extent permitted by law, if a bank receives a mortgage application from an applicant who is buying a home, the bank might share that fact with an *affiliated* insurance agency that sells homeowner's coverage. In these cases, the applicant is usually happy to receive timely information on insurance options and appreciates the "one-stop-shopping" capabilities that are made possible by responsible information-sharing within the corporate family.

This is not to suggest, however, that every institution shares information for marketing purposes. Indeed, a number of our member institutions have decided to refrain altogether from sharing information for marketing purposes (or have limited sharing). These institutions are trying to appeal to a segment of the marketplace that places a high priority on the privacy of customer information (e.g., those customers who do not want information shared even if it means the loss of potential benefits). The different approaches adopted by different institutions helps to highlight the natural byproducts of competition in a free market system. The end result is that consumers have different choices because consumers demand those choices.

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

There are many different reasons (or "purposes") for sharing information with *nonaffiliated* third parties. In most cases, the information is being shared to help the institution underwrite, process or administer a transaction that has been initiated by a consumer (e.g., sharing with data processors, credit bureaus, lawyers, accountants, etc.). In other cases, information might be shared because it is required by law (e.g., pursuant to lawful subpoena,

regulatory exams, etc.) or is necessary to prevent fraud. Most of these purposes are included within the "exceptions" contained in sections 14 and 15 of the privacy regulations promulgated by the FDIC, OCC, OTS, SEC and FTC pursuant to Title V of the Gramm-Leach-Bliley Act of 1999 ("GLBA Regulations").

In some cases, financial institutions will also share information with nonaffiliated third parties for marketing purposes. For example, in certain instances, a bank might provide information to an outside third party who performs services to help the bank market its own products or services (e.g., delivering customer names and addresses to a mailing house that helps to assemble and mail the bank's marketing literature).

In other cases, a financial institution might provide information to another nonaffiliated *financial institution* to help promote a financial product or service (i.e., pursuant to a so-called *joint marketing agreement*). For example, a bank might provide customer names and addresses to a broker-dealer in a so-called contractual networking program. That information might be used by the broker-dealer to provide the bank's customers with information concerning securities products in which they might be interested.

These types of "networking" programs are often used by smaller community banks to emulate the one-stop-shopping capabilities of their larger competitors (who do the same using *affiliated* broker-dealers). In these networking programs, the customer service representatives ("CSRs") are located in the lobby of the bank branch and interact almost exclusively with bank customers. The CSRs are often "dually employed" (employed both by the bank and by the broker-dealer) so that they can offer both banking products (e.g., deposit accounts) and securities products (e.g., mutual funds). Thus, for example, when a certificate of deposit is about to mature, the customer service representative can call or write the customer to offer him/her opportunities to roll the CD into another insured deposit product or possibly invest in a higher yielding, uninsured mutual fund. This type of "one-stop-shopping" environment has been applauded by many customers. Indeed, many of our member institutions report that their customers expect that the CSRs will have access to information concerning both their banking and their securities relationships. They want the CSRs to see their complete deposit/investment picture so that they can better advise them as to opportunities, risks, returns, etc. To satisfy that expectation, information must be shared between the broker-dealer (which manages the securities relationships) and the bank (which manages the deposit relationships).

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

The CBA's member institutions care deeply about the confidentiality and security of the nonpublic personal information of their customers. For that reason, many of these institutions often go well beyond the minimum requirements of the law and voluntarily place limitations on the sharing of information with affiliated and nonaffiliated third parties.

These limitations are quite varied and difficult to generalize. As is discussed above, financial institutions often consider a variety of factors when deciding whether information might be shared. Those factors include, among others, the sensitivity of the information, the

purpose for which the information is proposed to be shared, the nature and identity of the proposed recipient, the benefits available to the customer and concerns for the expectations of customers.

Within this framework, many of our member institutions choose, for example, to refrain from sharing information (or limit information sharing) for marketing purposes. Indeed, the vast majority of our member institutions do not share information with nonaffiliated third parties in a manner that would give rise to GLBA opt-out rights (e.g., they do not sell information to telemarketers or other mass marketers). Similarly, many of our member institutions do not share information with affiliates in a manner that would give rise to opt-out rights under the FCRA. Again, these variations in information management practices help to highlight the fact that consumers have choices. Those choices are driven by consumer demand and competition; not by law.

g. For what other purposes would financial institutions like to share information but currently do not? What benefits would financial institutions derive from sharing information for those purposes? What currently prevents or inhibits such sharing of information?

Currently, many smaller community banking institutions in Connecticut are not able to engage in certain information sharing practices that facilitate a one-stop-shopping approach to customer service for banking, securities and insurance products. Those limitations are often a product of state law. By way of example, here in Connecticut, state law prohibits a bank from sharing deposit information with third parties without the prior authorization of the customer.[4] This prohibition inhibits, among other things, the ability of a bank and broker-dealer to offer so-called "combined relationship" account statements that show deposit account information side-by-side with securities account information. The Connecticut opt-in requirement compels the maintenance of two separate (and expensive) monthly statement systems.

In contrast, some of the larger financial institutions are able to overcome the restraints of state law by using the preemption provision available under the FCRA (i.e., preempting state laws that restrict the sharing of information among affiliated entities). In these cases, these institutions are able to share information among affiliated entities in order to provide consumers with the benefits of one-stop-shopping services (e.g., the combined relationship account statement described above). As is discussed in section 6a, many smaller member institutions would like the same capabilities.

Finally, we note that the USA Patriot Act contains provisions which were intended to allow institutions to share information among themselves in order to prevent and detect crimes. The CBA is concerned that those provisions are not broad enough and might not provide an adequate safe harbor for institutions that wish to share information. Financial institutions continue to be interested in sharing information in order to detect and prevent crimes. We encourage the Department to work with the industry to find ways to achieve that goal.

[4] Last week, the Connecticut legislature amended this "opt-in" statute to provide, among other things, a limited "opt-out" provision for securities networking programs. That bill is currently awaiting the Governor's signature.

2. The Extent and Adequacy of Security Protections for Such Information.

a. Describe the kinds of safeguards that financial institutions have in place to protect the security of information.

The banking industry in Connecticut has taken great pains to protect the security of customer information. Those efforts include administrative, technical and physical safeguards that infiltrate virtually all operational areas within a bank. Those efforts also include measures that are designed to protect the security of information that is provided to affiliated and nonaffiliated third parties.

b. To what extent are the safeguards described above required under existing law, such as the GLBA?

Many of these safeguards are required under existing law or supervisory guidance. However, it should be noted that many of these safeguards were in place well before the GLBA requirements became effective.

c. What, if any, new or revised statutory or regulatory protections would be useful?

As a general rule, we do not believe that additional statutory or regulatory protections are necessary at this time. We do, however, continue to believe that the penalties against fraud (and other crimes against banks) need to be enforced and possibly made more stringent.

In addition, we believe that consumers can and should play a valuable (first defense) role in the prevention process. We encourage the government to increase its educational initiatives to enhance the likelihood that consumers will be able to protect themselves against identity theft, fraud and other security related crimes.

3. The Potential Risks for Customer Privacy of Such Sharing of Information.

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

There is always a "potential" risk whenever information is shared with any third party. We believe that the banking industry has done a good job of minimizing the risks that customer information will be misused by affiliates. This has been accomplished through the implementation of comprehensive privacy and security policies throughout the corporate family. In many cases, the risks, if any, created by the sharing of information among affiliates is equivalent to the risks created when information is shared within the institution itself (i.e., with another division or down the hall). Often, the affiliates share facilities and employees. This enhances the ability of the institution to place controls on the use and distribution of the information.

b. What, if any, potential privacy risks does a customer face when a financial institution shares the customer's information with nonaffiliated third parties?

Again, there is always "potential" risk whenever information is shared with any third party. However, we believe that the banking industry has done a good job of minimizing those risks through a variety of measures. Those risks are managed through careful selection of third parties and, where warranted, oversight of those third parties. Agreements with third party service providers contain covenants concerning security safeguards. Moreover, networking agreements with third party financial institutions (e.g., broker-dealers involved in joint marketing arrangements) contain assurances concerning information security and strict restrictions on reuse and redisclosure of information. The third party financial institutions involved in networking agreements (particularly with community banks) often act as the functional equivalent of an affiliate (with shared employees, shared space, etc.). As a result, banks are often in a good position to manage information use and distribution.

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?

Given the comprehensive implementation of policies throughout the corporate family (as discussed in section 3a above), we believe that the risks are managed in the same manner (and with the same degree of effectiveness) as is discussed in section 3b above.

4. The Potential Benefits for Financial Institutions and Affiliates of Such Sharing of Information.

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

Just as a bank needs to share information within the institution (e.g., among divisions and departments) in order to serve a customer with multiple relationships, a bank sometimes needs to share information with affiliates in order to enhance the one-stop-shopping experience. We note that certain financial services are required, by law, to be delivered by separate, functionally regulated entities (e.g., securities activities are required to be "pushed-out" to a separate, registered broker-dealer). But for the legal requirements for separate, functionally regulated entities, these related financial activities would be delivered under one corporate roof and information would be shared only within the same entity (e.g., among departments and divisions).

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

Many institutions need to outsource functions to nonaffiliated third parties. This is particularly true for smaller financial institutions that do not have the resources to perform all the functions that are necessary to service their customers' needs and operate their business.

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

In many cases, the benefits are similar to those enjoyed by divisions or departments within the same institution.

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

In the same manner as discussed in section 4b above.

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

Further limitations are not likely to be beneficial for financial institutions or their customers. Financial institutions and their affiliates need to have the ability to outsource functions and to share information to allow the functions to be performed (similar to the way in which information would be shared if all functions were performed within the institution).

5. The Potential Benefits for Customers of Such Sharing of Information.

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

There are many benefits available to consumers from information sharing with affiliates and nonaffiliates.

Among other things, responsible information sharing leads to lower cost products and services that can be delivered more efficiently. Greater access to information means better underwriting of loan products, which, in turn, leads to reduced portfolio losses (and this ultimately leads to lower rates and fees for customers). Greater access to information allows for faster processing of transactions.

Sharing information among affiliated entities as well as among nonaffiliated financial institutions involved in "networking arrangements" allows consumers to enjoy the benefits of a one-stop-shopping environment for the delivery of many different financial products and services.

Responsible sharing of information reduces blind telemarketing calls and "junk mail". Information sharing increases the potential for institutions to target customers with marketing initiatives that match customer needs or interests. It also allows marketing initiatives to be timed

to correspond to periods when the individual needs or wants the product or service. Customer response rates suggest that many customers appreciate well timed, targeted marketing initiatives.

Financial institutions often provide customers with special pricing or benefits when multiple relationships are maintained. If the various entities that provide the different relationships are unable to talk to each other about the relationships, customers will be denied the special pricing or benefits.

In many cases, those benefits are provided through affiliate relationships. In other cases, the benefits are provided through relationships among nonaffiliated third parties (particularly for smaller community banks).

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

The benefits are similar to those discussed in section 5b above.

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

We are not aware of any reasonable alternatives.

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

We believe that further legal restrictions would limit the ability of financial institutions to provide the benefits discussed above in sections 5a and b.

6. The Adequacy of Existing Laws to Protect Customer Privacy.

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?

As a general rule, we believe that the existing protections are adequate to protect consumers. Although complex, the existing federal privacy law matrix reflects a careful balancing of interests. The framework provides for disclosures concerning privacy practices so that consumers can make informed choices to utilize institutions that have adopted information management practices that best match their personal preferences. The law prohibits inappropriate disclosure and use of customer information, but, at the same time, provides important exceptions to allow financial institutions to conduct their business operations and to provide important benefits to consumers. The law provides an "opt-out" choice for consumers who do not want their information shared with third parties outside of the exceptions discussed above.

We submit that this new, balanced framework ought to be given time to work. For the most part, we have only experienced the first round of privacy notices, and the American public (and the nation's financial institutions) have not yet had the opportunity to fully digest and utilize the opportunities and choices provided by the law. We are convinced that if there is a demand for particular privacy practices, the financial services industry (or segments of the industry) will respond to that demand. As early evidence of this proposition, we point to the institutions that have already started to promote the fact (in their privacy notices and in their advertisements) that their customers' names, addresses and telephone numbers will not, under any circumstances, be shared with a telemarketer. We urge you to encourage Congress to let this framework mature so that we can truly see the benefits of a competitive marketplace.

Notwithstanding our "general" desire to preserve the existing federal law framework, we must object to the current framework for state regulation of privacy. Individual state actions have the potential to frustrate the consumer benefits currently available under the federal framework. With each state acting in its own unique way (e.g., Connecticut currently has several opt-in requirements), the end result is a complex patchwork of non-uniform laws across the country.[5] This, in turn, results in incredible expense for the industry (which inevitably gets passed along to customers) and non-uniform practices for multi-state operations. In some cases, variations in privacy practices (as a result of state law concerns) are so complex that they defy plain language explanation in privacy notices.

Given the foregoing concerns, we applaud the approach that Congress took under the FCRA to preempt state laws that restrict the exchange of information among affiliated entities. We **strongly** believe that the FCRA preemption provision should be made permanent (beyond its 2004 sunset date). Moreover, we **strongly** believe that the preemption provision should be broadened to encompass the information sharing scenarios contemplated by the GLBA joint marketing exception. That joint marketing exception was enacted to provide competitive parity for community financial institutions that are not large enough to serve their customers' needs through "affiliated" financial institutions. To compete and survive, smaller banking institutions need to have the ability to engage in contractual networking arrangements with broker-dealers, investment advisors, insurance companies, insurance agents, etc. To provide the benefits that consumers are demanding (i.e., the one-stop-shopping opportunities provided by their larger competitors), community banks need to share information with their networking partners (in the same way that affiliates are permitted to share). Under the current framework, the individual states have the ability to prevent information sharing among nonaffiliated entities. This represents a major competitive disadvantage for community banks. It threatens their survival and ultimately denies their customers the benefits of responsible information sharing. As is mentioned elsewhere, our community bank members tell us that their customers *expect* that information will be shared among the networking partners.

[5] We note that Connecticut alone has several different privacy laws. These include laws that are applicable to certain banking operations as well as laws that are applicable to insurance operations. These laws are not necessarily uniform in their approach to privacy protection (i.e., they are not consistent with each other or the federal framework).

We also encourage the expansion of the provisions of the FCRA that permit the sharing of "other information" (non-experience or non-transaction information). Those provisions currently allow for the sharing of such information among "affiliated" entities, subject to an opt-out right. That provision should be expanded to allow for the sharing of "other information" among *nonaffiliated* entities involved in networking or outsourcing relationships (subject to the same opt-out right). These types of entities typically perform the same types of functions as "affiliated" entities and the same set of rules should apply. As is discussed elsewhere in this letter, consumers benefit when information is shared among networking entities. Current law inhibits the availability of those benefits (particularly for community bank customers).

b. What, if any, new or revised statutory or regulatory protections would be useful to protect customers?

See the discussion set forth in section 6a above concerning the extension and expansion of the FCRA provisions.

7. The Adequacy of Financial Institutions Privacy Policy and Privacy Rights Disclosure Under Existing Law.

a. Have financial institution privacy notices been adequate in light of existing requirements?

We believe, in general, that the financial services industry has produced privacy notices that comply with the letter and spirit of the GLBA regulations. We note that many of our member institutions are currently trying to improve upon those privacy notices (based on customer feedback). We urge you to give the industry time to react to customer feedback before considering the implementation of new statutory or regulatory requirements.

We applaud the "workshops" that have been sponsored by the supervisory agencies. We hope and expect that those workshops will continue to produce a constructive dialogue on ways to improve notices. We are intrigued by the "short-form" notice concept that seems to be emerging from the workshop discussions. As those concepts evolve, we encourage the regulators to consider ways to provide a "safe-harbor" for the utilization of a short-form notice (i.e., providing comfort that a financial institution will not be held liable for failing to address required disclosures in more detail).

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?

We believe that new "requirements" are not warranted at this time. As is discussed above, we believe that the current framework should be given a chance to work.

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.

As is discussed above, we believe that the current federal framework reflects an appropriate balancing of interests. We do not believe that new "opt-in" requirements (or a broadening of "opt-out" requirements) is warranted.

Given current Connecticut law, many of our member institutions have actual, first-hand experience with the implementation of an opt-in program. Without exception, those member institutions report that the opt-in programs are cumbersome and expensive to administer. Those expenses ultimately get passed along to customers. They report that customers are often confused with the complexity of the opt-in rights (e.g., where it applies, where it does not apply), notwithstanding good faith attempts to provide plain language explanations in privacy notices and "consent" documentation. These institutions are concerned that their product offerings look clumsy and cumbersome when compared to those of their larger competitors (who use the FCRA preemption provision to share information with affiliates without regard to state opt-in requirements). We note that some of our member institutions have refrained from providing certain benefits to their customers simply because an opt-in program is too expensive and cumbersome to administer.

We believe, with certain exceptions, that broad-based opt-in requirements do not reflect a proper balancing of consumer interests and concerns. Studies suggest that most consumers are willing to allow information to be shared in a responsible manner if that sharing will produce lower cost products (or innovative services). Obtaining customer consent is a slow and cumbersome process that ultimately leaves many consumers with unexercised rights to opt-in. This is because the "default" position of an opt-in system operates to prevent the sharing of information. In the end, unless a consumer takes affirmative action to change the default position, the consumer never receives the lower cost product or innovative service.

We believe that the "opt-out" requirements that currently exist under federal law reflect a proper balancing of consumer interests and concerns. For the reasons discussed above, we would not support a broadening of opt-out rights in the affiliate sharing context.

We hope that our comments have been helpful. We appreciate the opportunity to comment and urge you to call me ((860) 677-5060), or our legal counsel (David J. Wiese of Tyler Cooper & Alcorn, LLP - - (860) 725-6213) if you have any questions.

Sincerely,

/s/ Lindsey R. Pinkham

Lindsey R. Pinkham
Senior Vice President