23

April 23, 2002

Regulations and Legislation Division
Chief Counsel's Office
Office of Thrift Supervision
Washington, D.C. 20552
(via electronic mail)

Attention: Comments on the GLBA Information Sharing Study

Ladies and Gentlemen:

Wells Fargo & Company ("Wells Fargo") welcomes the opportunity to comment on the Study on Information Sharing Practices Among Financial Institutions and Their Affiliates. Wells Fargo is a diversified financial holding company with over 30 subsidiary banks and over 100 additional subsidiaries that provide financial products and services to consumers. At the outset, I would like to point out that Wells Fargo does not share customer information with non-affiliates for the purpose of marketing non-financial products or services. Thus, our experience and the comments below are limited to the sharing of customer information with other financial institutions and service providers within the financial services industry.

The relatively free flow of customer information within the financial services industry in the United States has provided consumers with a selection of financial products and services that is unavailable anywhere else in the world. That same information flow has helped to increase competition in the U.S. financial services industry resulting in lower prices and greater customer convenience. In short, information sharing in the financial services industry has produced tremendous benefits for consumers.

The "consumer privacy risks" usually ascribed to information sharing really break down into three very different categories:

1. Risk of fraud, including identity theft, resulting in financial harm to the consumer;

2. Risk of unwanted intrusions, particularly telemarketing calls; and

3. Risk of inappropriate use of certain types of data, e.g., medical information obtained in connection with insurance products being used in credit decisions.

On close examination, it becomes evident that these risks are generally not increased by the *sharing* of information between legitimate businesses within the financial services industry. On the contrary, information sharing within the financial services industry can reduce the risk of

fraud and the incidence of unwanted intrusions. Information sharing also improves the accuracy and depth of customer data. While concerns about accuracy are not generally thought of as a "privacy" risk (although they do fall squarely within the term "data protection" used in much of the rest of the world), an increase in "privacy" at the expense of accuracy would be seen as a bad bargain by most consumers. Concerns about particular uses of particular kinds of data are better dealt with through restrictions on *use* rather than restrictions on *sharing*.

Our responses to your specific questions follow.

1. PURPOSES FOR THE SHARING OF INFORMATION

Customer information is shared, both among affiliates and with non-affiliates, for a variety of reasons:

(a) *To process transactions initiated by the customer*

Many transactions inherently involve parties in addition to the financial institution and its customers. For example, a routine check or credit card payment by the customer to a merchant necessarily discloses significant information to the merchant, the merchant's bank and the clearing or interchange system. Both the merchant's bank and the customer's bank are likely to use outside service providers as part of this process. There is, or course, nothing new about the information sharing inherent in various payments systems. However, it illustrates the point that customers routinely place "confidential" information into the stream of commerce without much thought as to the consequent disclosures of that information.

(b) *To service customer accounts*

Most financial institutions outsource many of their back office routing functions. In some cases these service providers are affiliates; in many they are non-affiliates. In addition, most customers are not aware of and do not care about the often complex subsidiary structures of many financial institutions. Customers of Wells Fargo Bank Minnesota expect to be able to transact business and obtain information at Wells Fargo Bank Wisconsin—or Wells Fargo Bank Alaska—just as easily as at their local Wells Fargo branch in Minneapolis.

(c) *To prevent and detect fraud and to control risk*

Consumers in the United States enjoy tremendous benefits from the existence of a nationwide market for financial services in terms of choice, cost and convenience. Many consumers can obtain instant credit, for even a major purchase such as an automobile, from a variety of lenders—often based in other states—even during evening or weekend hours. Lenders can prudently offer credit to borrowers they have never met because of the quality of the information in our consumer credit reporting system. That information comes primarily from the financial institutions that already have experience with those individuals. Other databases

contain information that enables financial institutions to verify the identity of a customer or check for suspected fraud. Again, much of that information originates from other financial institutions. While much of the data used to control credit and fraud risks is provided through third-party databases, financial institutions also exchange information for these purposes directly with each other, especially in the case of affiliated institutions. This can eliminate the delay and costs inherent in posting information to, and retrieving it from, a third-party database.

(d) *To market complementary financial products*

If only because of regulatory constraints, no single legal entity can, on its own, actually deliver to consumers a complete array of financial products and services. Nevertheless, being able to offer our customers all the financial products and services they need is the mission of Wells Fargo, and many of its competitors.

Besides banks, we have a mortgage company, a consumer financial company, securities broker-dealers, insurance agencies, financial consultants and tax preparers. Subject to our customers' information sharing and solicitation preferences, we may share most types of customer data—other than medical information—among these affiliates so that, on an enterprise-wide basis, we can offer the full array of financial products and services appropriate to the circumstances of each customer. However, unlike some of our competitors, Wells Fargo does not have consumer insurance underwriting capability. Because insurance is an important part of most consumers' financial portfolio, we have joint marketing agreements with a number of insurance companies under which we share customer information, subject to the customer's right under our own policy to opt out of such sharing. Because these "partners" may also be, or be affiliated with, competitors in other markets, the information shared is limited to that which is required for them to make underwriting decisions, and subject to contractual restrictions on other uses. In addition, many direct marketing functions in connection with the products and services we offer directly are outsourced to nonaffiliated service providers. Service providers are generally given the minimum customer information required for them to successfully perform their assigned functions.

(e) *To meet legal and regulatory requirements*

Customer information is routinely shared with non-affiliates, including government agencies, to meet legal and regulatory requirements, respond to legal process, etc.

(f) *Wells Fargo voluntarily limits information sharing*

Note: The following description of Wells Fargo's current policies and practices is provided or purposes of this comment letter only and is not intended to confer any rights in addition to or contrary to those described in its official consumer privacy disclosures.

(i) Except as may be required by law, Wells Fargo does not use or share medical information for any purposes unless expressly authorized by the consumer.

(ii) Wells Fargo permits customers to opt out of all affiliate sharing for marketing purposes even though the FCRA does not require an opt out for identifying or "transaction and experience" information.

(iii) Wells Fargo permits customers to opt out of information sharing under joint marketing agreements with non-affiliated financial institutions even though GLBA does not require such an opt out.

(iv) Wells Fargo does not share customer information with non-affiliates for the purpose of marketing non-financial products or services without the customer's express consent, even though GLBA would permit such sharing subject to an opt out.

(v) Wells Fargo permits current customers to request "do not call", "do not mail", "do not e-mail" and "do not solicit" (by any means) status even though existing laws generally cover only telephone solicitations, and generally exempt calls to current customers.

2. EXISTING SECURITY PROTECTIONS FOR CUSTOMER INFORMATION ARE ADEQUATE

Protecting the "privacy" of customers is an important goal, but probably not the controlling factor in developing a financial institution's security systems and procedures. If customer information is compromised, the financial institution will likely bear most or all of any financial loss, as well as suffer from a loss of goodwill and adverse publicity. Misuse or negligent compromise of customer information by a joint marketing partner or service provider may have all of these negative consequences, as well as lead to competitive harm. Accordingly, the level of protection of customer information is driven primarily by safety and soundness concerns rather than compliance issues. While the documentation of information security procedures required to comply with the Guidelines Establishing Standards for Safeguarding Customer Information adopted pursuant to Section 501(b) of GLBA was a useful exercise, compliance with GLBA and the Guidelines has not had a significant impact on the substance of our information security policies or practices.

3. PRIVACY RISKS ARE NOT INCREASED BY INFORMATION SHARING

As noted in our introductory remarks, three very different types of "privacy" risks are generally ascribed to information sharing, each of which must be separately analyzed.

(a) *Risk of financial loss due to fraud*

Various kinds of fraud, especially identity theft, are serious concerns for both consumers and financial institutions. However, there is little if any evidence to suggest that planned information sharing—with affiliates, non-affiliated financial joint marketing partners or service providers—is a significant contributor to this problem. Most identity theft can be traced to theft of information (a) directly from the consumer—e.g. by theft of a wallet or purse; (b) in the course of transactions initiated by the consumer—e.g., "dumpster diving" by merchant employees or others; or (c) by interception of communications between the consumer and the institution—e.g., theft of statements or pre-approved offers from the consumer's mailbox. Due diligence in the selection and monitoring of marketing partners and service providers is a necessary precaution, but probably can prevent only a small percentage of fraud losses. On the other hand, the free flow of information among affiliates and throughout the financial services industry is essential to the prevention and detection of fraud, including identity theft.

(b) *Risk of unwanted intrusions*

If asked to describe specific "privacy" concerns, most consumers would probably put telemarketing and "junk" mail at the head of their lists. At the same time, American consumers continue to spend billions of dollars every year in response to telephone and direct mail solicitations. In reality, a solicitation is junk mail—or an unwanted phone call—only if it is selling something in which the recipient has no interest. It is entirely possible to carry on a mail or telephone campaign with virtually no information about the members of the target audience. Information sharing enables limiting such campaigns to those who are most likely to be interested in and qualified for the product or service being sold. Company-specific "do not call" lists such as those required by the Telephone Consumer Protection Act and blanket "do not call" lists such as those maintained by many states (and currently proposed by the Federal Trade Commission on a nationwide basis) provide more effective protection from unwanted intrusions than restrictions on information sharing. Indeed, restrictions on information sharing would be counterproductive in this regard, since less targeted marketing would result in more solicitations in which the recipient has no interest.

(c) *Risk of inappropriate use of certain types of data*

Ever since the Citi-Travelers merger was announced, the specter of medical information obtained in connection with insurance coverage or claims being used to deny credit applications has haunted the debate over sharing information among affiliates. We know of no evidence that any lender has ever used medical information obtained from an insurance affiliate in making credit decisions. In fact, it is unlikely that any lending and insurance affiliates have achieved the level of integration of customer information systems that would be required to do that in a systematic way. Under other circumstances, consideration of medical information by an affiliate might well be in the customer's best interests. For example, some investment products might be inappropriate for someone with a short life expectancy. And, to return to more realistic

examples of affiliate sharing, it is obvious that a complete picture of a customer's financial situation—including banking, investment and insurance products—is useful, if not essential, in helping the customer make sound financial decisions going forward. If there are concerns about particular uses of specific types of data, they should be addressed by restricting how such data may be used (as has been done, for example, in the Equal Credit Opportunity Act and the Fair Housing Act) and not by sweeping restrictions on information sharing.

As noted above, Wells Fargo is exclusively in the financial services business, and restricts information sharing to (a) its affiliates, (b) other financial institutions providing complementary financial products and services, (c) affinity and private label partners and (d) service providers to financial institutions. We do not believe that customer "privacy" risks are materially different depending on the identity of the recipient of customer information within this limited set; we have no experience beyond this set and thus express no opinion as to potential risks if information is shared outside the financial services industry.

4. BENEFITS OF INFORMATION SHARING FOR FINANCIAL INSTITUTIONS

As noted above, financial institutions and their affiliates benefit from sharing information internally by having a more complete picture of the customer's financial circumstances which enables them, on an enterprise-wide basis, to better meet the customer's expectations in terms of service, to take advantage of cross-sell opportunities and to manage their own risks and resources more efficiently. Information sharing with non-affiliated financial joint marketing partners enables the financial institution to offer products and services which it cannot provide directly while still maintaining control over the customer relationship. Information sharing with service providers enables the financial institution to concentrate on its core competencies while leveraging the expertise and capacity of the service provider to provide better service at lower cost than if the same functions were performed in-house. Further limitations on information sharing would degrade the level of service than financial institutions can provide to their customers, increase their operating expenses and expose them to greater levels of risk.

5. BENEFITS OF INFORMATION SHARING FOR CUSTOMERS

Information sharing—among affiliates and with financial marketing partners—provides customers with one-stop shopping for their financial service needs, lower costs reflecting lower operating expenses and improved risk assessment, and the convenience of being able to conduct banking and other financial transactions in many locations, sometimes nationwide. Sharing of information with non-affiliated service providers has reduced the cost of financial services by improving operating efficiencies, fostered nationwide competition further reducing customers' costs while increasing their options in terms of products and providers, and enabled such conveniences as nationwide and even global ATM networks and instant credit. Further restrictions on information sharing would degrade customer service and convenience, reduce choices and increase costs.

6. EXISTING LAWS ARE ADEQUATE TO PROTECT CUSTOMER PRIVACY

FCRA effectively precludes financial institutions from sharing with non-affiliates information other than that arising from their own "transactions and experience" with the customer. FCRA also permits customers to "opt out" of sharing such "other" information with affiliates. GLBA requires financial institutions to disclose their information sharing policies and practices and to permit customers to "opt out" of information sharing with non-affiliates, subject to prescribed exceptions. Other laws protect customers from liability for fraudulent charges, punish identity theft and restrict unwanted telemarketing calls. The current legislative and regulatory scheme has been in effect for less than a year. While some continue to complain about "inadequate privacy protection," there have been few, if any, instances where it is possible to identify a specific harm that is not addressed by existing laws and regulations.

7. SIGNIFICANT IMPROVEMENTS IN PRIVACY DISCLOSURE WILL REQUIRE REGULATORY CHANGES AND CONSUMER EDUCATION

Many of the privacy disclosures sent in 2001 have been criticized as confusing and hard to read, and we agree that improvements can and should be made. However, much of the blame must fall on the complexity of the disclosures mandated by the GLBA privacy regulations and the use of "safe harbor" language found in those regulations. Many companies, including Wells Fargo, are moving toward simpler disclosures even if that means foregoing the protection of the sample language in the regulations. However, the regulations themselves still require a level of detail and complexity that goes beyond what most consumers can really understand or care about. Revising the regulations to eliminate some of the required complexity may be a necessary step to achieve notices that are truly comprehensible by the average consumer. Another factor contributing to consumer confusion is that few of them have any understanding of the uses and disclosures of consumer information that are part of providing financial products and services. Thus, they lack the proper context to understand the scope and implications of the choices available to them under GLBA and FCRA. Until the level of consumer knowledge improves—and that will require more than mandated disclosures—making notices easier to read will not guarantee that they are really understood.

8. "OPT IN" REQUIREMENTS WILL INCREASE COST AND REDUCE CONSUMER CHOICES

"Opt in" has a superficial appeal in that it supposedly gives consumers "more control" over how information about them is used. However, that extra measure of control is beneficial only if consumers truly understand the consequences of failing to opt in. The reality is that, under an opt in regime, it becomes prohibitively expensive to present certain alternatives to consumers in the first place. In 1992, Vermont enacted a law that effectively eliminated prescreened credit offers as of January 1, 1993. Certainly the Vermont legislature thought it had provided its citizens with a greater level of protection with respect to their credit report data.

Because the economics of non-prescreened (or "invitation to apply") solicitations are less favorable, some credit grantors simply excluded the entire state of Vermont from programs extending credit. When the citizens of Vermont discovered the opportunities they were missing (because they heard about them from friends and relatives in neighboring states), the law was repealed on April 9, 1993, less than 100 days after it had gone into effect. If opt in is adopted at a national level, some offers simply will not be made at all.

The notion of permitting customers to "opt out" of all sharing of information among affiliates ignores the fact that information not now subject to opt out under FCRA, "transaction and experience" information, is generated as a result of the interactions between the customer and the financial institution; it is *not* solely the customer's information. Further restrictions on affiliate sharing would increase the cost of providing financial services and impair the ability of financial institutions to understand and serve their customers' financial needs. Such restrictions would also impede efforts to prevent and detect fraud and assist law enforcement agencies. Even if there is an exemption for disclosures made for fraud control and law enforcement purposes, it is unlikely that financial institutions will design and develop information systems to take advantage of such exemptions if those capabilities provide no revenue enhancement opportunities but do present a compliance risk.

Finally, we would point out that any mixture of opt in and opt out would inevitably make privacy disclosures and choice notices even more confusing than they already are.

9. PERMITTING CUSTOMERS TO RESTRICT SHARING FOR PARTICULAR USES IS NOT FEASIBLE

Wells Fargo, like many other financial institutions, voluntarily restricts the use and sharing of particular types of information (e.g., medical information) and does not permit sharing of information for certain purposes (e.g., marketing of non-financial products and services). We also permit customers to request "do not call", "do not mail", or "do not solicit" status, which effectively blocks the use of information for such purposes. However, we do not believe it is feasible to provide customers with more extensive options to restrict sharing of particular types of information or sharing for particular purposes. Providing such a menu of choices would require extensive systems enhancements, introducing significant additional complexity into both those systems and the procedures of the financial institutions. Presenting such choices in privacy disclosures and choice notices would increase the complexity and thus potential for confusion in such documents, and that would be contrary to the widespread desire to simplify these notices. In addition, offering a plethora of choices would result in many consumers not making the correct choices to achieve the results they intend; we already know that many consumers opt out of information sharing when they really want to achieve "do not solicit" status.

Please feel free to contact the undersigned at (415) 396-0940 or by email at mccorkpl@wellsfargo.com if you have any questions regarding the foregoing comments.

Very truly yours,

PETER L. MCCORKELL

Peter L. McCorkell
Senior Counsel
Wells Fargo & Company