Remarks by
Julie L. Williams
Chief Counsel
Office of the Comptroller of the Currency
before the
Financial Institutions Insurance Association
Regulatory and Compliance Conference
June 22, 1999

When this conference was being scheduled several months ago, my topic was listed as -- "Guarding Consumer Privacy: Understanding the Guidelines for Sharing Customer Data." Little did any of us know, that the timing of this speech would coincide with the explosion of privacy as an issue in the debate on financial modernization legislation, litigation challenging a major financial firm's privacy practices in connection with telemarketing, and a surge of privacy-related stories in the media.

This morning I will first recap recent developments that have shaped the privacy debate for the financial services industry. Then I will cover the status of regulatory and legislative responses as well as the role of the marketplace in safeguarding privacy. I will conclude with a snapshot of where we are today and dust off some old, but still relevant perspectives on the issue of privacy.

It would require an extraordinary set of blinders not to recognize that American consumers are increasingly privacy conscious. Survey data bear out that consumers are concerned about threats to their privacy and about whether they have lost control of information they consider personal and private. Interestingly, whereas in the past, customers seemed to be most concerned about government intrusions into their privacy, current customer concerns about privacy appear to be greatest in the areas of private sector uses of financial and health information.

When a privacy issue -- identity theft -- is the premise for a hit movie starring Sandra Bullock -- *The Net* -- I do not think it is productive to continue to debate whether privacy is a major consumer issue, or to suggest that customer concerns are merely "anecdotal." The question must be, rather, how the issue can be credibly addressed, and how fast that can be done.

Privacy abuses touch a common nerve. They may come in the form of the inconvenience of dealing with a telemarketing call at dinner time; having to empty a mailbox full of unwanted catalogues; finding a plethora of identifying information about yourself on the Internet; the sudden appearance of unexplained credit card charges; having your bank account robbed by way of a forged check; having your identity stolen; or being stalked. Each of these is a breach of personal privacy -- ranging in severity from mere irritants to crimes that incite fear for personal safety. They are not academic or remote occurrences. We can identify with their victims.

It is against this backdrop -- this increasingly charged atmosphere where each new reported invasion of personal privacy triggers a visceral, public reaction -- that I would like to reflect on the topic of privacy and the privacy challenges you are facing in your businesses.

In part, we have arrived at this point in the privacy debate because of the explosion of information technology. Technological advances have greatly facilitated the collection, dissection, and transfer of vast amounts of personal data. Information can be sliced, diced and shared at a level of personal detail that was never before possible. These new capabilities have turned personal information into a marketable commodity, and cause consumers -- when they learn about it -- to question whether highly personal medical and financial information should be in the hands of, and exploited by, third parties.

There are two sides to the commoditization of information. Businesses, armed with extensive data about individual preferences and circumstances, can profit by tailoring products and services to maximize their appeal to consumers. A banker recently told me about his company's goal of customizing and individualizing credit cards to appeal to a market of one. Bankers talk about the ability to anticipate and satisfy their customers' changing financial needs over the course of a lifetime. It is the availability of these opportunities that may well cement relationships between customers and their financial institutions. In short, personal information is a potent and profitable tool in a company's portfolio -- when used responsibly.

The pace and magnitude of mergers and affiliations in the financial services industry fuel the privacy debate. Moreover, Congress is currently considering legislation that would enhance the ability of different types of financial services companies to affiliate, thereby increasing the potential for gathering and using personal financial and medical information about the company's customers.

One key rationale for these combinations is that resulting companies will be able to "warehouse" data on an expanded customer pool and "mine" that data to design an increasing array of targeted and profitable product and service offerings. Affiliations among diverse sectors of the financial services industry are intended to create new synergies and opportunities for cross marketing to customers. Again, this ability is heavily reliant on sharing and pooling data. The shear magnitude of these data warehouses and the sensitivity of the information they hold fuels public skepticism and anxiety about the security and proper uses of such data and propels Congress to devise safeguards to protect against its misuse.

That gets us to the heart of the privacy debate -- both the perception and the reality that individuals are losing control over their personal information. When the information is highly sensitive, such as medical and financial information, consumer concern about who has control over its disposition is compounded. And that leads me to the other part of the privacy equation -- the industry's response.

Curiously, given the importance of information as a valuable business asset, the financial services industry has been more defensive than proactive in its reactions to date to customer privacy issues. Frankly, I find this somewhat surprising given the virulence of the industry's opposition to the proposed Know Your Customer rule on grounds that it would lead to unwarranted intrusions on customer privacy. The attitude of at least some industry representatives has been -- show me the harm, show me the complaints. The problem with this attitude is that, in many instances, individuals may not realize -- and have no way of forcing disclosure of -- just how their personal information is being handled. However, as daylight begins to shine on firms' practices for handling customers' personal information, the public appears ready to make a stink about the shortcomings they see. Any company that ignores, or fails to understand the tinderbox of public sentiment waiting to ignite on privacy, acts at its peril.

An example comes to mind that the Comptroller spoke about two weeks ago -- the exchange of extensive confidential customer information by a bank and its insurance affiliate to an unaffiliated telemarketer in return for commissions on sales made by the marketing firm to bank customers. Imagine how customers reacted when they learned from press accounts of a lawsuit filed by a state Attorney General that alleged that their trusted financial institution had sold their name, address, phone number, social security number, account number, account balance, last payment date, occupation, marital status and much more, to a telemarketer. A telemarketer. I'll tell you how they reacted. They phoned in complaints in droves. They lined up at the bank to demand an explanation, and in some cases, to close their accounts.

Commendably, senior management of the bank reacted swiftly. In a newspaper add directed at its customers the bank announced, "There is nothing we value more than the trust you put in us. When that trust is called into question it's something we take very seriously." The bank announced that it would end its participation in all such marketing relationships.

This particular bank learned a very expensive lesson about respecting customer privacy. I certainly hope that other financial service providers are learning this same lesson derivatively, and not waiting to get burned.

I'd like to take a moment to comment on the proliferation of bank privacy policies. I commend the banking trade groups for promulgating privacy principles and urging their members to adapt and adopt such principles. Many, many banks have heeded the call -- more and more banks are posting privacy policies on their web sites. It is essential, however, that these steps be more than window-dressing. Privacy policies are meaningful only if they reflect an organizational commitment, are adhered to, are stated in terms customers can readily understand, and meet legitimate customer expectations about the handling of their personal information.

As many of you know, the banking regulators have also weighed in on this debate. At the OCC, we have been gently, and perhaps sometimes not so gently, prodding the industry to get its privacy house in order. We have issued guidance to the

industry in areas such as safeguarding customer data from unauthorized release to unscrupulous information brokers or "pretext callers" posing as bank customers. Where there are relevant privacy laws, we have taken steps to encourage banks to scrupulously adhere to them. Last March, the OCC issued guidance to national banks about effective practices for meeting the notice and opt out requirements for affiliate information sharing under the Fair Credit Reporting Act. Most recently, in May, again through the issuance of effective practices guidance, we encouraged banks to establish privacy policies and post them on their web sites. We are currently considering mechanisms to ensure that banks maintain adequate procedures and internal controls to enhance compliance with stated privacy policies.

Pressure on the privacy front is further being exerted by the states through legislation restricting the uses of customer information, and lawsuits, such as the one I noted that was filed two weeks ago, that also seek to stem the flow of customer information. Also, Congress presently has pending many bills concerning the treatment of personal information -- most of which are aimed squarely at the financial services industry. The evolution of the privacy debate surrounding consideration of financial services modernization legislation reveals what a potent issue privacy has become.

In the last Congress, discussions of privacy were at the periphery of the debate over modernizing the financial services industry. Privacy legislation affecting the industry that was either enacted into law, or came close to passage in the last Congress, was aimed at data security -- such as curbing identity theft which is now law, or punishing pretext callers who obtain confidential information from banks under false pretenses. The dynamics have shifted dramatically over the course of this year, however.

In March, the House Banking Committee had an unexpectedly long and vigorous debate over an amendment offered by a freshman Congressman that would have required banks to notify customers about their information sharing practices with third parties and an opportunity to opt out of the sharing of that information. Members reacted viscerally to descriptions of current practices and the limited reach of existing privacy laws. But, by the next day, after Committee Members were "educated" by the industry, many had set aside their gut reactions and spoke about operational difficulties and unknown consequences of increased restrictions on the transfer of customer information. The amendment failed, and in its place, the Committee adopted an amendment requiring disclosure of privacy policies.

When the Senate considered S.900, its financial modernization bill, in the beginning of May, privacy amendments were generally fended off. A number of pro-privacy Senators announced that the issue should be considered separate and apart from S.900. That view largely prevailed.

But just weeks ago, the issue resonated when the House Commerce Committee considered H.R. 10. A Commerce subcommittee adopted a measure mandating that financial services companies disclose their information sharing practices to their customers. However, by June, a growing clamor to address existing and potential privacy

abuses resulted in the passage of an amendment that requires financial services companies to provide their customers with the opportunity to opt out of all types of information sharing arrangements with unaffiliated and affiliated third parties.

It remains to be seen whether some type of enhanced privacy protections will be retained in financial modernization legislation as it continues to move through the Congress. But, it is evident that the marketplace has already begun to recognize the significance of distinctions in privacy protections afforded consumers. There is evidence that -- when information is available -- market forces will take privacy issues into account. Just last week, a large bank announced that it was taking an "industry-leading" privacy position by ceasing the sharing of customer information with third party marketers. In doing so, the bank said that "customer privacy is one of our highest priorities."

That brings me to my last point -- where do we go from here? The financial services industry is just beginning to realize the potential of the Internet and the business opportunities made available by technology. But these very developments increase the potential for intrusions on personal privacy and facilitate the transfer of personal data. And, as more information about how customer information is collected and used becomes available, market forces increasingly will take privacy consequences into account.

I would offer one suggestion today for how the financial services industry can approach this challenge. It is not a solution, but rather an attitude, drawn from Justice Louis Brandeis' eloquent description -- over seventy years ago -- of the concept of privacy. He called it "the right to be left alone -- the most comprehensive of rights, and the right most valued by a free people." These words capture an issue central to treatment of privacy concerns in the new information age.

Privacy as an individual right implies that to some degree personal and private information about an individual is the property of *that individual*. That also implies that when a customer gives that property to another for one express purpose, he or she is not implicitly giving it for whatever other purposes the recipient may want to use it.

My suggestion is to think of personal information from your customers' perspective, as something they feel belongs to *them*. In developing and implementing privacy policies, think about how you customers would react if you gave them a full description of how much of their information you collect, what you do with it, whether you transfer it, who you transfer it to, and what happens to it then.

Would you be embarrassed?

Would your customers feel they have been treated fairly?

Structure your privacy policies -- and implement them -- accordingly.

Thank you.