Remarks by

Julie L. Williams
Acting Comptroller of the Currency

before the

Banking Roundtable Lawyers Council
Washington, D.C.

May 8, 1998

It is a great pleasure to be here this morning with you to discuss a topic that is significant for the banking industry today, and will be even more so in the future -- customer information and personal privacy. This subject has come into the spotlight with the recently proposed megabanks and financial services conglomerates, as well as with the continuing advances in electronic banking and commerce. The banking organizations that comprise the Bankers Roundtable -- the largest banking organizations in the country -- are particularly likely to possess large amounts of information about very large numbers of customers. And you, in your role as counsel to these organizations, have the potential to influence how your company deals with this precious information resource.

I thought, therefore, that I would offer my perspectives on this issue -- an issue that is already commanding significant attention in our increasingly information-driven economy.

My premise is a very simple one. The banking industry needs to demonstrate leadership in the treatment of confidential customer information and personal privacy issues. Otherwise, it risks a customer backlash that could fuel reactions at the federal and state levels that lead to restrictions on your ability to use precious information resources.

You have much at stake here. The latest developments in the financial world underscore the importance of information-sharing for consumers and providers of financial services alike. One key rationale for the recently announced megamergers in financial services is that the resulting companies will be able to gather and distill data on an expanded customer pool, and use that data to design better, more efficient product and service offerings to meet individual customer needs -- for example, offering advice and products to help consumers realize bigger returns on their savings, build assets for retirement, and obtain ancillary products, like property insurance, at the same time and place that they secure financing for that property. Another rationale for these mergers is to provide more convenient access to existing and potential bank customers. This geographic expansion probably means more sophisticated data warehousing that can result in low-cost access to new, perhaps custom-tailored product and service offerings for bank customers. In both situations -- expansion by scope or scale -- we're seeing a natural marriage of technology and relationship banking, and it's one reason why these mergers look so attractive

from the vantage point of the constituent companies. In the best case, we have a win-win situation: new business and new synergies for financial institutions, more choice and more convenience for consumers.

But it's not simply in connection with the cross-selling of products and services and data collection and storage that information management can provide real benefits for consumers of financial services. The Internet and personal computing have brought many banking transactions into the home -- a special boon for our aging population and for all of us leading too-busy lives. Recent advances in the availability of credit -- especially to segments of the population formerly viewed as less creditworthy -- may be traceable in large part to the growing sophistication of the credit analysis and reporting business, which is now able to gather more complete and more accurate information on potential borrowers and help lenders better control and price risk. Surveys show that consumers recognize that financial institutions have a legitimate need for personal information to make rational credit decisions, and that consumers generally are willing to provide that information for such purposes.

But the same surveys also reveal growing anxiety about how personal information is being used and, in some cases, misused. The media regularly bring us tales of individuals whose lives have been disrupted by fraudulent use of social security numbers, bank and credit card account information, real estate recordation, and even medical records and other nonfinancial data, much of which can be gathered without special authorization and without violating any current law. Consumers are discovering the limits of confidentiality and the absence of effective protections against the determined thief, hacker, or snoop. There is little doubt that privacy concerns today are slowing widespread acceptance of electronic commerce generally and electronic banking particularly.

The seriousness of these concerns was a key finding of the Consumer Electronic Payments Task Force, a group which Treasury Secretary Rubin asked the OCC to chair back in 1996 and whose final report was released last week. The report's focus is on "e-money," but the questions we heard from consumer representatives during the Task Force's investigations speak to the broader issue of financial privacy. First, consumers want adequate disclosure about a company's information collection and use policies. Secondly, they don't want to have to reveal more information than is needed for a transaction. And, finally, they are also concerned about the use of that information for purposes other than the original transaction, either by the information collector or by a third party to whom the information is sold or transferred.

Interestingly, while we heard a few calls for sweeping new laws that would involve the government more directly in the electronic marketplace, that was a decidedly minority opinion. Most of what we heard was consistent with a market-oriented policy toward electronic commerce. This is also the approach of the Administration's "Framework for Global Electronic Commerce," which articulated five basic principles to govern this fast-developing part of our economy. Those principles include private sector leadership; the avoidance of undue government restrictions; predictable government involvement where necessary;

respect for the decentralized nature of the electronic marketplace; and the minimization of international barriers to electronic exchange.

The recommendations of the Consumer Electronic Payments Task Force are consistent with this general approach. In the area of privacy, we call for meaningful and effective industry self-regulation -- self-regulation that responds to consumers' privacy concerns, provides disclosure to consumers about privacy policies, and offers some means to assure compliance with these policies. The report also suggests that the industry explore ways, through the use of technology, to provide consumers with greater control over the collection and use of information pertaining to them and their financial transactions.

Industry self-regulation has the potential to address many consumer privacy concerns.
But, although I am hopeful, as a bank regulator, I am a paid skeptic. And if self-regulatory initiatives are viewed as weak and toothless, the stage will be set for a more active government role.

Indeed, we are already seeing growing government interest in this issue -- movement the financial services industry should view as a signal that pressure is beginning to build. In a very short time, the Federal Trade Commission will be delivering a report on privacy to the Congress, and, separately, the Commerce Department is due to deliver to a report on online privacy to the President. The Clinton Administration has also focused on privacy issues raised in connection with electronic commerce. And just last week, the House Commerce Committee opened a series of hearings on electronic commerce in which privacy was a recurring theme. Assurances from industry representatives that self-regulation was sufficient to eradicate abuses met with some skepticism.

Your course should be clear. It is emphatically in the interests of the financial services
industry -- whose basic raw material, after all, is information -- to take the lead in demonstrating that self-regulation can and will work, and that public concerns about privacy can be addressed without requiring externally-imposed government solutions to the problem.

What I would like to do in my remaining minutes here today is to comment on the industry's self-regulatory efforts to date and suggest how, from a regulator's perspective, we might make better use of the laws already on the books to deal with some of the privacy concerns we are hearing from consumers.

For the last several years, the financial services industry has been hastening to address the public's heightened interest in privacy. In 1995, Mastercard issued a statement assuring customers of privacy protection, and Visa soon followed suit. The following year, the American Bankers Association (ABA) issued a report underscoring the privacy obligations of the banking industry. In May 1997, the SmartCard Forum issued its "Guide to Responsible Consumer Information Practices." And in September of last year, the Banking Industry Technology Secretariat -- the B-I-T-S -- of the Bankers Roundtable adopted a far-reaching set of privacy principles, later endorsed by the Roundtable itself, the American Bankers Association, the Consumer Bankers

Association, and the Independent Bankers Association of America.

The BITS principles are intended to apply to all phases of a consumer's banking relationship, and not just to electronic transactions. They include a recognition of the customer's expectation of privacy, limitations on the use, collection and retention of customer information, control over employee access to that information, restrictions on sharing of account information, disclosure of an institution's privacy policies, the consumer's right to "opt-out" of any information-sharing arrangement, and more. The Bankers Roundtable is to be commended for sponsoring this important work.

But while principles like the BITS principles certainly move us in the right direction, I believe that additional steps need to be taken if those or any other principles that the industry chooses to adopt are to lead to truly effective self-regulation in the banking industry. My major concern centers on the lack of means to assure adherence to the principles. Principles may call on banks to establish internal procedures to ensure compliance with the bank's own privacy policies, but who will judge whether a bank's policies are consistent with a particular set of industry self-regulatory principles or whether they are being complied with? What remedies will be available to deal with those institutions that fall short of the standards?

These questions are relevant not just to privacy policies applicable to electronic banking and electronic commerce, but to the treatment of confidential customer information generally. It seems essential that self-regulation in the privacy area must have teeth in order to be credible. For example, other self-regulated industries in the United States retain independent auditors to check on the level of compliance with the industry's own standards and principles; in European countries, there are consumer ombudsmen whose job it is to resolve complaints, including those related to privacy. It may be that the banking industry needs to consider similar arrangements. But if, for whatever reason, banking organizations decline to adopt industry-wide policing, it is especially important that the market be allowed to operate through full disclosure of privacy policies. In the coming years, as former FTC Commissioner Christine Varney has noted, "privacy may well become a market commodity," and third parties could find a commercial niche comparing the privacy policies of competing banks and advising consumers on where their privacy is most likely to be respected and safeguarded.

To understand why enforcement matters so much, let's look at a related area -- compliance with the 1996 amendments to the Fair Credit Reporting Act (FCRA), which affects the use of consumer information. Congress passed these amendments in response to industry concerns about pre-existing limitations on their use of select credit bureau information and about restrictions on their ability to share and use information among companies within the same corporate family, such as affiliates and subsidiaries. The amendments greatly enhanced market opportunities for business. Congress revised the rules, granting banks more flexibility in their use of credit bureau information, and expanded the scope of permissible information-sharing among affiliates.

But consumer privacy was a key political consideration in the final agreement to liberalize the rules, and Congress required that consumers be given the right to request that their information not be used. For credit bureau information, a credit bureau and any business that typically accesses credit bureau information in advance of communicating with consumers, must inform those consumers contacted that they have the right to exclude their name from any future information requests for two years. In the affiliate information-sharing area, an institution that wants to share information with a related company may do so free of restrictions placed on credit bureaus, provided that the consumer receives advance notice and opportunity to direct that the information not be shared. In other words, consumers have the right to "opt out" of any information-sharing arrangements.

But, unfortunately, it has been known to happen that the affiliate-sharing "opt out" disclosure is buried in the middle or near the end of a multi-page account agreement. For existing accounts, some institutions have gotten into the habit of reducing the required "opt out" disclosures to the fine print along with a long list of other required disclosures. Few consumers are likely to have the fortitude to wade through this mass of legal verbiage, and fewer still will take the time to write the required "opt out" letter. I have even heard of people getting two separate notifications covering different types of information, requiring two separate letters to opt out. Such techniques may fall within the letter of the law, but they certainly fall short of its spirit.

On the other hand, I have seen evidence of responsible consumer notification and opportunity to opt out. In one case, the bank sent its customers a separate letter informing them of the benefits, by way of greater product and service availability, that resulted from the sharing of customer information among affiliates, but also providing a detachable form for their customers to use to opt out. This type of simple, straightforward, and convenient approach should be embraced by the banking industry.

If, however, the industry is perceived as failing to administer the opt out process in an unambiguous, straightforward way, public pressure could build to impose new regulatory standards or to broaden the banking agencies' ability to examine banking organizations regarding their implementation of the opt out process. With respect to the latter, as a result of the 1996 amendments to the FCRA, the federal banking agencies are currently authorized to conduct examinations under two circumstances: when a specific consumer complaint is received or when the supervisory agency "otherwise has knowledge" of a FCRA violation. We believe that the second circumstance applies to knowledge of FCRA violations obtained in the normal course of a review for compliance with other laws and regulations, and we intend shortly to release specific guidance to clarify this point for bankers and examiners.

In closing, let me emphasize that government, the private sector, consumer and other voluntary organizations all have important parts to play in implementing the benefits of cross-selling and

targeted marketing and the convenience of new technologies, while preserving social and personal values. Privacy remains one of those basic values. The banking industry today has a rare opportunity to step up to the plate and become a leader on the critical issue of personal privacy and responsible customer information practices -- an issue upon which so much of the industry's long term future depends.

Thank you.