Remarks by
Julie L. Williams
Acting Comptroller of the Currency
before the
Consumer Bankers Association
Aventura, Florida
October 26, 1998

Thank you and good morning. It is a pleasure to join you here in Aventura, where I trust that, in the company of the sunshine and your peers, you will enjoy some deserved relief from the strains and aggravations that are too often the lot of consumer bankers these days.

I suspect that no one here today was around when the CBA was first established back in 1919, but those of you with years in the business under your belts will recall a time when banking was a good deal less complicated and more predictable, and when the future of the banking franchise was not clouded by the competitive and technological challenges that bankers face today.

Yet, while some might lament the passing of that simpler age, it is irretrievably gone. Today's world is a place of relentless change and competition, of unforgiving markets and customers who have no compunction about taking their business elsewhere. The nature of competition itself is in constant flux. Where it was once enough to match up against the financial institution across the street or across town, your customers' business today is up for grabs from competitors across the nation and, in some cases, around the world. And, as you know, the competition has become more sophisticated in identifying and appealing to consumer tastes and preferences. While it is certainly true that financial products and services are priced and sold more like commodities than ever before, I firmly believe that it is a serious misconception to think that intangibles -- such as service, security, and convenience -- no longer matter to consumers. In fact, as securitization and wider competition make the financial marketplace more uniform, it seems likely that those intangibles will become even more prominent on the battleground of future competition.

Let's call them "competitive intangibles," and focus on one in particular: customer

privacy and information security. Rarely has an issue landed in our midst with more dramatic impact. And when it comes to privacy, have no doubt that banking -- the quintessential information-driven industry -- cannot avoid the spotlight.

The Consumer Bankers Association has long recognized this and has worked actively on privacy issues affecting the banking industry. Over many years, the industry has set -- and achieved -- high standards for safeguarding confidential data and has built an impressive reservoir of consumer trust.

But today, some worry that banks have not reacted quickly enough to emerging customer concerns and new risks to customer privacy brought on by rapid advancement in technology and the "commoditization" of personal information. In recent Congressional hearings, information brokers and pretext callers revealed the shocking ease with which they were able to pry loose personal financial information from overly-accommodating bank customer service personnel. Banks are themselves leading users and traders of their customers' personal information. Indeed, the recent wave of mergers in the banking business is explicitly motivated in part by opportunities to gather and distill data -- "mining" in the current phraseology -- on an expanded customer pool.

Three impressions emerge from the current attention to the privacy issue. First, public concerns about the proper -- and improper -- accumulation and use of personal information are likely to increase with the continued explosive growth of electronic commerce and the Internet. Second, providers that go the extra mile to satisfy these concerns will be at a material advantage over those that do not. And third, to the extent that business is perceived as not living up to customer expectations regarding the use and safekeeping of personal information, pressure will continue to build for government action that could lead to restrictions on your ability to use precious information resources.

Although the information revolution has surely heightened these concerns, technology has long been viewed as a challenge to privacy. So, the sensitivity of customers to this issue should not come as a surprise. It is easy to forget that 1984, George Orwell's nightmare vision of a technologically-sophisticated Big Brother, was published almost fifty years ago.

As longstanding leaders in the introduction of technology to the marketplace, bankers are not unfamiliar with the challenge of making consumers comfortable with innovations that alter the way business is traditionally conducted. Credit cards and automated teller machines are success stories whose importance should not be overlooked, for they illustrate that, even where something as fundamental as money is concerned, consumers are willing to accept change in return for perceived benefits -- in this case, greater access, convenience, and choice. Consumers want the chance to realize bigger returns on their savings and investments. They want the opportunity to obtain ancillary banking products and financial products tailored to their specific needs and desires. And they recognize that, in order to deliver those products, financial institutions have a legitimate need for relevant information about their customers.

In short, consumers want what bankers are increasingly in a position to offer, thanks in large part to advances in information technology. But what customers clearly don't want are unpleasant surprises that undermine the trust and confidence they place in banks. They don't want their personal information to be used for unanticipated or undesired purposes, and they want to be confident that their information will not be misappropriated from the bank by other parties.

Shortly after becoming Acting Comptroller, I convened a Privacy Working Group within the OCC, and asked it to look at the performance of national banks in addressing various privacy issues. Although the group's work continues on, it has already identified some developments that I want to share with you today.

Most of the banks we have spoken to have adopted privacy policies and promises, usually modeled on the eight principles recently adopted by the leading bank trade organizations, including the Consumer Bankers Association. Among these principles are recognition of the customer's expectation of privacy, limitations on the use, collection, and retention of customer information, control over bank employee access to that information, and more. Most banks that have websites list and sometimes discuss their privacy policies. This kind of disclosure represents

a growing and encouraging trend.

However, when I last spoke on the subject of privacy, back in May, I emphasized that outside parties with a stake in the privacy debate -- public interest organizations, members of Congress, and the regulatory agencies -- would be closely monitoring the extent to which financial institutions were actually embracing and implementing the industry's principles. Information developed by our working group suggests that there is room for improvement in this respect. More banks need to adopt or adapt explicit internal policies and procedures to implement their own privacy principles. Others will need to perform a more comprehensive review of their existing policies and procedures to make certain that they are consistent with their new statements on privacy and information confidentiality. In some cases, employee training will need to be refocused on privacy issues, to ensure that policies are understood and respected.

Another focus of our working group has been on industry compliance with the so-called "opt-out" affiliate information sharing procedure in the Fair Credit Reporting Act, known as FCRA. The pertinent provisions of that act require that banks provide "clear and conspicuous" notification to customers explaining that they will share information with affiliates unless consumers exercise their right to opt out.

When I delivered my May privacy speech, I reported anecdotal evidence that some financial institutions were not in compliance with the letter or the spirit -- or both -- of the FCRA provisions. Our Privacy Working Group indicates that this is still too often the case. We can find too many disclosure statements that lack specificity, clarity, and simplicity. They are too often opaque and obscure, rather than "clear and conspicuous. " They place the burden on customers to provide a long list of information, including, in at least one case, account numbers for each account for which information is not to be shared. Too often we found disclosure information in fine print, buried in a mass of equally tiny type, along with other required terms and disclosures.

In short, we continue to find that consumer anxieties -- based on the lack of clarity and consistency in banks' disclosure policies and practices -- are not entirely unfounded.

Certainly, while banks have come a long way in addressing consumers' concerns, they clearly have more work to do in this area. Information sharing that is open and honest can be a boon for both banks and consumers.

Indeed, as I suggested at the outset of my remarks, privacy has increasingly become a competitive issue. Former Federal Trade Commissioner Christine Varney suggested that "in the Information Age, privacy may well become a market commodity" in global commerce. And in Europe, the treatment of consumer privacy has advanced well beyond that.

This month -- yesterday, in fact -- the European Union's privacy directive went into effect. Predicated on the idea that privacy is a basic human right, this directive imposes a high standard of protection for consumers dealing with financial and other firms in the nations of the EU. The directive requires that consumers get disclosure statements on how personal information will be used and the option of preventing companies from sharing information about them. Furthermore, the EU directive gives consumers specific legal remedies in case personal information is misused. And it expressly prohibits the transfer of personal data out of the EU to a third country unless that country ensures an adequate level of privacy protection. Right now, the United States is not on the list of countries that meet the European standard.

The EU directive does make allowance for special contractual arrangements with individual financial institutions, arrangements that would allow them to continue doing business in the EU as long as EU-conducted audits find these institutions to be in essential compliance with national privacy laws. The adoption of practices that meet European privacy standards would not only permit U.S. institutions to continue doing business in the EU, but could also have the effect of promoting higher privacy standards for financial institutions operating in the United States.

Just because EU policies are right for Europe does not necessarily make them right for the United States. Each of us has unique traditions, customs, and values. Yet privacy is clearly an issue that American consumers care about. They do today and they always have. Therefore, the way in which U.S. banks recognize and react to privacy-related

concerns, such as how confidential consumer information is used and how it is protected from misappropriation, can be a "competitive intangible -- either an asset or a liability -- depending on the bank's actions. Given what we know about the level of consumer anxiety about privacy, when this issue is handled well, it can become a powerful marketing tool and an important source of customer loyalty.

When I testified before Congress on privacy issues in July, I told the House banking committee that all of us -- lawmakers, regulators, and bankers -- were in it together in meeting the public's demand for convenience, safety, and privacy in their financial dealings. At the OCC, we have worked to advance the joint privacy interests of banks and consumers. In cooperation with other Federal regulatory and law enforcement agencies, we issued an advisory letter to national banks, alerting them to the dangers of pretext phone calling and identifying appropriate steps by which to better safeguard customer information. We promulgated new policies to clarify our ability to examine national banks for FCRA compliance. Soon, we expect to release "best practices" guidance for banks on two subjects: website disclosures and implementation of privacy principles and promises, and disclosures and practices for the affiliate information-sharing procedures under FCRA. And just last week, we convened a Privacy Forum, which brought together representatives of the financial services industry, consumer groups, and government staff to discuss many of the issues I have raised here this morning.

We have also cooperated with Congress to strengthen the legal framework for dealing with those whose actions undermine public confidence in financial privacy. Now awaiting the President's signature is the Identity Theft and Assumption Deterrence Act of 1998, which criminalizes identity theft, gives victims the ability to seek restitution, and establishes in the Federal Trade Commission a central clearinghouse to receive complaints and assist victims. When it is signed, this law will help us to arrest what is today one of the fastest growing types of financial fraud.

Not enacted by Congress but hopefully ripe for passage in the next Congress is a bill, the Financial Information Privacy Act, that would establish sanctions for unscrupulous

information brokers who "steal" confidential customer information from financial institutions through techniques such as pretext calling.

Yet, although regulators and lawmakers have important roles to play in safeguarding the confidentiality of consumer financial information, the primary burden rests with you who have the most to gain from it. In our free market economy, that is as it should be. It continues to be the position of our government that the best way to advance the interests of the American people in a free and unfettered flow of information and goods and services lies in applying the minimum amount of regulation and government intervention that is consistent with the public welfare. Just how much intervention that involves will depend upon the steps that the industry takes to establish and implement its own policies and principles in the coming months.

Self regulation offers banks the ability to shape their own policies and avoid being subject to the one-size-fits-all approach that might be mandated under the law, while still effectively addressing customers' privacy concerns. Through enlightened self regulation, banks can preserve access to customer information without impinging on customers' right to privacy. And that will help ensure that our information-driven banking system remains safe, sound, and competitive in the years to come. So I urge you, in each of your institutions, to act vigorously to demonstrate that the banking industry can make self regulation work.

Thank you.