Remarks by
John C. Dugan
Comptroller of the Currency
Before the
ALI-ABA Financial Services Institute
Washington, D.C.
February 2, 2006

Good afternoon, it's great to be with you. I have often attended this conference, but today is special for me because this is my first opportunity to speak to this group in my capacity as Comptroller of the Currency. Or, looked at another way, this is my first speech to a legal conference as a *client*, which is how our Chief Counsel's office thinks of me. If you're like I was in private practice – occasionally gritting your teeth after cranky phone calls from the people you represent – you may have fantasized about what life would be like on the other side. Well, I've now been here six months as a client, and I'm here to tell you that, despite your fantasies, despite all the headaches that go with being the lawyer, being the client . . . *is great!* I love being the client. Who wouldn't love being the boss of a bunch of smart lawyers who do excellent work?

But seriously, being the client, rather than the counselor, hasn't diminished my interest in the legal issues affecting the banking system. Nearly every day presents a challenging mix of policy, supervisory, and safety and soundness matters that intersect with legal issues. The topics I'll highlight this afternoon – privacy and information security – are two such matters that hold the promise of important regulatory and legislative developments emerging in the year to come.

Before doing that, however, I would be remiss in addressing this audience if I did not at least touch on national bank preemption. Although this issue has not been as much in the news

lately, it remains as important as ever to the national banking system. As you know, recent court decisions have been remarkably consistent in finding that particular types of state laws aimed at national banking activities are preempted. I have been especially pleased with the recognition in a number of these decisions of the reasonableness of the OCC's position in interpreting the authority that Congress has entrusted to the agency in the National Bank Act. The Second Circuit's opinion in *Wachovia v. Burke* is a good example of this. The Court found that OCC regulations "reflect a consistent and well-reasoned approach to preempting state regulation of operating subsidiaries so as to avoid interference with national banks' exercise of their powers under [the National Bank Act] and their ability to use operating subsidiaries in the dynamic market of banking and real estate lending." Likewise, the federal district court in the *OCC v. Spitzer* case repeatedly described the OCC's positions as reasonable and consistent with the purpose and intent of the National Bank Act.

Time will tell, of course, but I like to think that, after a period of intense controversy, these and other decisions reflect a growing consensus about the uniform federal standards that form the core of the national banking system. The corollary principle, which I fully recognize, is that the OCC shoulders a unique responsibility in implementing a federal regulatory regime that applies credibly and uniformly to banks operating in every part of the country. What I've learned in my first six months at the agency is that we are dedicated to carrying out that responsibility every day.

Privacy Disclosures

Let me shift gears now and talk about privacy – a consumer concern that has been a major issue for the financial services industry, where some interesting developments may be in the offing. As required by the Gramm-Leach-Bliley Act, banks and other financial institutions

have been providing privacy notices to their customers since 2001. We know from surveys that most people don't bother to read these notices, even though most people report that they care about privacy. Fundamentally, these notices just don't appear to be especially useful to consumers.

I have some well-formed views about why this is true. When I was in private practice, I was very involved from the industry side in the process that produced Title V of Gramm-Leach-Bliley, and later, its implementing regulations. I also participated in an effort sponsored by the entire financial services industry, which was never completed, to develop a template for more "user friendly" financial privacy notices that would comply with Gramm-Leach-Bliley. And I testified on a number of privacy issues, including notices, before legislative committees in Congress and a number of states.

Based on this experience, I believe there are a number of reasons why privacy notices are not as useful as they should be. First, the statutory requirements, which reflect the first real effort by Congress to address financial privacy, are complex and mandate a host of very specific disclosures. That makes it hard to have short notices.

Second, while the regulations did a remarkably good job of translating the specific statutory requirements of Title V into a coherent framework, they could not escape some of their statutory constraints. Perhaps more importantly – some would say "sadly," though probably not this group – the notice requirements were drafted by lawyers. In the type of quest for legal precision with which I am all too familiar, this part of the regulations encouraged the use of legal terms in notices by including them in the sample clauses. Except in the case of warped privacy lawyers like me, "nonpublic personal information" and "nonaffiliated third parties" are not exactly household words.

Finally, although the statute and regulations require that certain topics be addressed in the notices, there is no requirement for uniformity or even consistency among different institutions in the way in which the information in the notices is presented.

When you combine these three factors, the result is what we have today: notices with too much information, too many legal terms, and too much variability in presentation from institution to institution. Each year, banks and other financial institutions bear the cost of mailing such mandatory notices to their many millions of customers, even though we suspect that most of the notices go from postman to trashcan without ever being read. Put more harshly, in too many instances privacy notices are nothing more than costly waste.

Can't we do better? Can't we find a way to deliver more useful information to consumers, and where appropriate, reduce the cost to financial institutions? I think we can. For example, on the cost point, I think there are certain circumstances in which it serves no useful purpose for institutions to mail privacy notices year after year. Specifically, if an institution does not share information in a way that would require it to give notice to a customer of his or her right to "opt out" of such sharing, then it seems to me that repeated annual notices are simply unnecessary; an initial notice and notices furnished upon request would be more than adequate. For this reason I strongly support the provision in the regulatory burden relief legislation that has passed the House Financial Services Committee that would make just such a change to the annual notice requirement in Gramm-Leach-Bliley.

More fundamentally, I was delighted to learn since assuming my new role that the federal banking agencies and the FTC are quite far along in a major effort to simplify financial privacy notices. As many of you know, in December 2003, the agencies issued an Advance Notice of Proposed Rulemaking outlining and seeking comment on a new approach to privacy notices –

one that would make these notices easier for consumers to understand and use. The agencies sought comment on sample versions of streamlined notices with key information presented in a simplified check-the-box or yes/no format. Perhaps most significantly, the agencies pledged to engage in consumer testing before proposing changes to the privacy regulations.

The agencies have since retained expert consultants to test privacy notices with consumers. The object of the testing is to assess weaknesses with current notices, suggest creative alternatives that correct these weaknesses, and test these alternatives with consumers. And the purpose of this latter testing, obviously, is to determine whether consumers find the notices useful – not just whether they like the way they look. For example, if a consumer wants to limit his bank's sharing of personal information, can he easily determine from the notice how to "opt out"? If a consumer wants to compare sharing practices among banks, can she easily do so based on the banks' notices?

Both banks and their customers can benefit from the use of simplified privacy notices, especially if they allow easy comparison of different banks' information sharing practices. Shorter, focused notices will lessen the burden on banks. They will also empower consumers to make informed decisions about their personal information. That could lead to more consumers opting out of information sharing, which banks might not like. But by the same token, if more customers actually read and understand privacy notices, banks will have new opportunities to market themselves based on the particular types of information sharing practices they choose to adopt – and I think that would be quite a positive development.

So stay tuned. I expect the testing project to provide valuable data about what consumers can understand and use to evaluate an institution's information practices. The testing results will inform the agencies' next steps in advancing the use of simplified notices. And whatever path

we propose to take, we will expect and welcome vigorous comment before any final changes are made.

Information Security

The second area I want to discuss today is often mentioned in the same breath as privacy, because it, too, concerns the appropriate use of consumers' personal information. It has also generated a tremendous amount of publicity in the last couple of years. I'm referring, of course, to information security, and specifically to the standards businesses should use to protect personal information; the types of businesses that must employ these standards; and the circumstances that should trigger mandatory notices to consumers about security breaches involving their personal information.

Banks and other financial institutions are already required by Title V of Gramm-Leach-Bliley to protect the security and confidentiality of customer information. Under joint banking agency guidelines issued in 2001, a bank must implement a comprehensive written information security program to protect customer information against anticipated threats and unauthorized access or use that could result in substantial harm or inconvenience to any customer. A bank must oversee service provider arrangements where service providers have access to or maintain customer information. This includes using due diligence in selecting the service provider and requiring service providers by contract to safeguard the bank's customer information. A bank's information security program must not be static, but should instead be adjusted to reflect changes in technology, new business arrangements, and new threats.

In March 2005, the banking agencies issued final guidance further interpreting the interagency guidelines. This requires banks to implement response programs that specify the actions an institution would take in the event of a security breach involving customer

information. The guidance also describes the circumstances under which institutions should notify their customers about breaches involving their personal information – mainly when there is a breach of security and evidence that the information has been or will be misused.

The guidance applies only to institutions that fall under the jurisdiction of the banking agencies and, indirectly, to their service providers. It does not apply to data brokers, merchant card processors, or retailers – all of which suffered well-publicized breaches last year, some involving account information of millions of consumers. There is no federal law that compels these companies to notify consumers of breaches involving their personal information.

Not so at the state level, where nearly half the states have laws that require companies to notify consumers of security breaches involving their personal information. These laws differ from each other, sometimes subtly, sometimes significantly: from the circumstances that trigger a breach notice to consumers, to the acceptable delivery mechanism for the notice.

Banks are subject to this patchwork of state requirements *and* the federal standard in the banking agency guidance. The Gramm-Leach-Bliley Act does not preempt state laws if they are not inconsistent with federal requirements. A state law is not inconsistent if it is more protective of any person than the federal standard, with the Federal Trade Commission as the final arbiter of what is more protective. Of course, it is not always clear which law is more protective. For instance, one state does not expressly allow a company to delay sending notices to consumers where law enforcement requests such a delay to avoid compromising a criminal investigation. The banking agency guidance does permit delayed notice in these circumstances. Which one of these standards is more protective – the one that permits law enforcement to conduct an investigation unimpeded, or the one that alerts consumers to the breach immediately?

Given the spate of well-publicized security breaches, the lack of a federal standard outside the financial services sector, and the patchwork treatment by the states, it is no surprise that Members of Congress have weighed in on the subject. They are certain to continue the debate during this legislative session. A handful of committees in the House and Senate are in various stages of considering legislation. Key issues include the type of personal information that should be protected; the standard for triggering notice when there is a security breach involving that information, including whether a company should have the discretion to determine the possibility of misuse before providing notice to consumers; the range of companies that should be covered; and the circumstances that should permit or dictate a delay in notice. There is also debate about which agencies should be authorized to write the rules, which should enforce the rules – and of course, whether and to what extent to preempt state laws.

These are complex issues to sort out, especially as they may have unique ramifications for banks. For example, as I mentioned earlier, banks are already subject to a robust set of information security requirements under Gramm-Leach-Bliley. These have been tailored to the unique circumstances of an industry that is extensively regulated and supervised. I believe that this regulatory regime has worked well, evidenced by the appropriate steps that a number of banks have taken in the past year to disclose and remedy security breaches that presented opportunities for abuse of compromised customer information. It is not clear whether this regime, which depends in part on the comprehensive supervisory authorities of the banking agencies and their role as examiners, would work well if extended to unregulated companies and industries. Conversely, it is equally unclear whether a one-size-fits-all standard designed for all companies would work well for regulated banks. What is clear, however, is that banks should not be subjected to two different federal standards. Either they should continue to be subject to

the Gramm-Leach-Bliley regime alone, with modifications as appropriate, or that regime should be supplanted by one that applies to all companies – so long as a standard can be crafted that makes sense to apply to bank and nonbank companies alike.

If Congress should take the latter route by adopting a single federal standard for all U.S. institutions, including banks, I believe that three principles should guide their actions:

First, functional regulators should write the rules for institutions within their jurisdiction. For banks, this would obviously be the federal banking agencies, since they are responsible for regulation, supervision, examination, and enforcement. These agencies have deep knowledge of banking operations and are therefore in the best position to implement legislative requirements in measured ways that are tailored to banks' unique circumstances.

Second, functional regulators should have exclusive authority to enforce these rules. Because of their comprehensive supervision and examination role with respect to banks, the federal banking agencies are best suited to detect violations of law, ensure compliance, and apply appropriate sanctions. The banking agencies also have a well-established array of enforcement tools that range from informal to formal actions, depending on the severity of the violation, and these have already been used effectively to enforce existing information security rules under Gramm-Leach-Bliley.

Third, I believe a uniform national standard is appropriate to govern the safeguarding of personal information and notice to consumers of security breaches. The maintenance and safeguarding of customer information is not defined by geographic boundaries. Information can be transferred by electronic means anywhere in the nation instantly, and may be physically transported from state to state and across the country. Customers typically do business with multiple financial institutions, many of which are not located in the same locale as the customer.

Moreover, it is very costly and burdensome – and may be impossible – for institutions that operate in multiple states, including both small and large companies, to comply with numerous and inconsistent state requirements. A strong uniform federal standard would provide sound protections for consumers, without imposing unnecessary burdens and confusion.

Conclusion

In closing, let me reiterate that privacy and security are just a sampling of the interesting issues we see in the financial services legal arena. These will present many challenges in the months and years to come, so I am delighted to have had this opportunity to share my thoughts with you today, during the early part of my tenure.

Thank you very much.