Remarks by
John D. Hawke, Jr.
Comptroller of the Currency
Before the
Institute of International Bankers
Washington, D.C.
March 5, 2001

The IIB's annual Washington conference has long been a highlight of the season, for me and for the Washington financial community, and I'm delighted to be speaking to you at such an eventful time for international bankers. The past year has seen a number of supervisory initiatives of real consequence for IIB members. But rather than surveying what is truly a broad field, I thought I'd focus in on one area that's engaged a considerable portion of my time and thought in recent months -- the supervisory challenges presented by Internet banking.

The rise of the Internet will certainly be remembered as one of the defining developments of our time. The financial services industry felt its effects early on, and in some parts of the industry the effects were far reaching. On-line trading of securities, which offered customers cost savings and convenience that traditional brokers were hard pressed to match, not only transformed the securities business but also helped drive the bull market that reached its peak last year. There's little doubt that the advent of on-line trading was a big factor in the increase in the number of Americans who have participated in these markets in recent years.

In the banking industry, the effects of the Internet have been less dramatic but scarcely less significant. Three years ago, only about 100 banks and thrifts offered any banking services over the Internet. Since then, the rate at which banks have "gone online" has been rapid, especially compared to the early phases of other technology-

based banking services, such as automated teller machines. Although five institutions have already been chartered by the OCC as Internet banks, the vast majority of banks that have embraced the Internet have done so as an additional delivery channel rather than as a stand-alone application. Today most banks see the development of online services as a major component of their business and marketing strategies, and are investing very significant resources in upgrading their technological capabilities and acquiring the human resources to effectively utilize those capabilities.

The dynamism of Internet banking is reflected in a recent OCC survey. It shows that 37 percent of all national banks allow customers to conduct financial transactions online -- nearly twice as many as were offering online transactional services only 15 months earlier. Twenty eight percent of national banks make account information available over the Internet. Thirty five percent of national banks still have no Internet presence, but they are invariably smaller banks that, in total, account for only 10 percent of all national bank customers. Even so, the number of national banks that are not online in some capacity is almost certain to drop, as bank customers increasingly come to expect on-line access to their financial information, regardless of the size of the institution they bank with.

Whether conducted as a stand-alone activity or as an adjunct to a traditional network of brick-and-mortar branches, Internet banking obviously poses some special risk management challenges for bankers and supervisors. For example, most banks outsource the technical design, installation, and maintenance of their Internet systems, choosing not to do themselves what others can probably do better and cheaper. But the relationship between the bank and the technology vendor takes on a new sensitivity in the

Internet environment. The more customers respond to marketing efforts and increase their reliance on bank web sites to conduct routine transactions remotely, the greater the bank's dependence on those who make those transactions possible. In such situations, banks have a great deal to lose -- reputationally and otherwise -- if the vendor's performance comes up short.

Security is another issue with serious implications for Internet banking providers. The risk of intrusions and security breaches has grown exponentially with the number of remote access devices and the availability of sophisticated tools that, in the wrong hands, can turn just about anyone with access to a PC into a dangerous hacker. And, with more and more sensitive information available online, computer criminals -- as likely to be motivated by politics or self-aggrandizement as material gain -- have greater incentive to cause mischief than ever before.

Finally, Internet banking presents unprecedented cross-border and international challenges for bankers and bank supervisors. It's this aspect of the Internet banking phenomenon that I'd like to focus on today.

We should begin by noting that the risks I've just mentioned -- a list intended to be suggestive rather than exhaustive -- are by no means unique to Internet banks. All financial institutions run risks associated with outsourcing and information security, whether or not they operate in the Internet environment. And all financial institutions that operate in the international environment -- as each of you well know -- have to deal with cross-border issues relating to such things as the political, economic and social values and habits of their transnational customers and the legal and regulatory frameworks of host countries.

The Basel Committee on Bank Supervision was born of the recognition that banks everywhere face common -- and increasingly interrelated -- risks. Since its establishment in 1974, the Committee's work can be understood in terms of two general goals. First, it has always had as its purpose to facilitate the exchange of ideas and the sharing of practices capable of being adapted to the special circumstances of each nation's supervisory system. Initially, the Committee's approach embraced a kind of non-judgmental agnosticism -- rejecting, if only by implication, the idea that any one supervisory approach was preferable to another, and operating from the presumption that the bank supervision that suited one nation might not suit another. But over the years, while by no means abandoning its deference to and respect for national differences, the Committee has evolved a commitment to common principles of supervision, aiming to harmonize global supervision and to establish minimum supervisory standards where necessary. The Committee's work on capital standards is perhaps the best known example of this approach.

Second, in a more active mode, the Committee has striven to become a deliberative body through which coordinated supervisory responses can be fashioned to situations that require them. Indeed, it should be remembered that the Committee had its genesis in the Bankhaus I.D. Herstatt incident of 1974 -- a relatively small bank whose failure had global repercussions. For bank supervisors, that event was a wake-up call, and from it came a new commitment to international cooperation, which was increasingly recognized as essential if the spillover effects of such disruptions were to be contained. Further, supervisors recognized that instability in the international setting was a two-way street -- that it could move from the provinces to the center, as it were, just as easily as

from the center outward, as was the case with Herstatt. Either way, cooperation among supervisors was crucial.

So the challenge of cross-border supervision was a big part of the Committee's raison d'être from the beginning, and an early focus of its work. In 1983, the Committee released a set of principles for the supervision of banks' foreign establishments, which was revised in 1992 and then again in 1996. These statements established four main principles:

- All international banks should be supervised by a home country authority that capably performs consolidated supervision and has the right to prohibit corporate structures that impede supervision;
- The creation of a cross-border banking establishment should receive the prior consent of both the host country and the home country authority;
- Home country authorities should possess the right to gather information from their cross-border banking establishments; and
- If the host country authority determines that any of these three standards is not being met, it could impose restrictive measures or prohibit the establishment of banking offices.

These principles, which use the respective roles of "home" and "host" country as the basis for developing cooperative cross-border bank supervision, provided significant comfort to host-country supervisors. They provided a reasonable basis for concluding that cross-border branches and subsidiaries licensed and supervised within their borders were being capably supervised by the parent bank's home-country supervisor.

But this guidance did not reckon with the Internet. The guidance was grounded in the assumption that cross-border banking will be carried out through a physical presence in the host country. It never contemplated the virtually unlimited capability of Internet banks to distribute products and services across national borders without a physical presence. It did not address the practical difficulties facing host country authorities that might wish to monitor or control Internet banking offerings originating in other jurisdictions, at least insofar as those offerings reached citizens of the host country. It did not take into account the potential ability of a bank or non-bank to use the Internet to cross borders and to seamlessly link banking activities that might be unsupervised by any financial market authority.

It was in response to these circumstances that the Basel Committee formed a subgroup, the Electronic Banking Group, or EBG, which it's my honor to chair. The EBG membership comprises 17 central banks and bank supervisory agencies from G-10 countries, along with a number of observers.

One of the EBG's first orders of business was to inventory and assess the major risks associated with e-banking. Those risks, we concluded, fall into six broad risk categories: strategic risk, legal risk, operational risk, country risk, reputational risk, and, finally, credit, market, and liquidity risk.

The EBG's catalogue of e-banking risks -- and the all-important question of how bankers and bank supervisors might best respond to those risks -- have largely defined the EBG's agenda over the past year. It's been a year of intensive research and study. We initiated an ambitious outreach and communication program with prominent private sector institutions active in e-banking developments and activities, including financial

institutions, third party service providers, and vendors. A series of Industry Roundtables, held in North America, Europe, and Asia, have allowed the EBG to obtain invaluable insight and information regarding e-banking risk issues, current strategic and product developments, and emerging risk management standards. It's been a lively and productive year.

Now, after digesting all that we've learned, the EBG has prepared a report entitled "Principles for Risk Management of Electronic Banking," which is in final draft and I expect will be released for public comment later this month. The theme of the report is that e-banking should be conducted with no less attention to the fundamentals of safety and soundness than banking activities conducted through traditional delivery channels. Our report presents 14 risk management principles, organized under three headings: Board and Management Oversight; Security Controls; and Legal and Reputational risk management.

In preparing this guidance, we have tried to be as specific as possible in alerting financial institutions and their supervisors to the nature of the risks they face in the e-banking environment and in suggesting sound practices to manage these risks. But we have also been mindful of the fact that each e-banking situation is different and may require its own customized approach to risk mitigation. Our expectation is that bankers will put these principles to use as they develop policies and procedures to govern their e-banking activities.

More recently, the EBG has turned its attention to developing guiding principles for cross-border cooperation among bank supervisors. In a study now underway, we're looking more specifically into the practical difficulties of applying the existing Basel

cross-border framework in the Internet environment, how home countries should go about supervising Internet banks, how host countries can be affected, how differing supervisory standards for Internet banks can be reconciled, and how home- and host-country supervision of these "virtual" banks might work. Finally, we're working to identify possible actions that the bank supervisory community can take to facilitate supervisory cooperation on cross-border Internet banking.

Since I've already offered a few examples of how Internet banking has complicated implementation of the existing Basel cross-border principles, let me give you some idea of where our thoughts are now headed in terms of what may be required to cope with the supervisory challenge of the virtual environment.

Our fundamental belief is that the responsibility for effective supervision of Internet banking -- even more than for brick-and-mortar banking -- rests with the home country supervisor. Home supervisors need to make certain that their banks understand the risks posed by Internet banking and how to manage these risks effectively. As I've mentioned, the EBG has dedicated considerable time and effort to that goal. Communicating supervisory expectations and procedures for overseeing Internet banking activity is essential both to help ensure that locally supervised banks properly manage risks and to help host supervisors understand the supervisory regime that the home supervisor uses for its institutions.

Where, then, does the host supervisor enter the picture? Is its role limited to placing its faith in the competence and good intentions of the home supervisor and hoping for the best? How do local policies on a whole variety of issues get taken into account? In the earlier world of physical banking, these were relatively easy issues, since

any institution working to establish a physical presence in a host state could be required to obtain a license that would expressly subject them to local laws and policies.

Needless to say, sound principles of cross-border supervision in the virtual world must address the role of host country supervision. While Internet banking certainly poses difficulties for the host country, the EBG is developing a progressive framework for host country supervisors to use if, for example, they become concerned about the legality or prudential nature of a foreign bank's Internet banking activities. This escalating approach would have the host country supervisor start by remonstrating with the foreign banking entity itself. If that proved unsuccessful, the supervisor would bring the problem to the attention of the home country supervisor. And if that too did not produce the desired results, the host supervisor would alert local consumers that the Internet banking entity was operating improperly. At the heart of this approach is the belief that supervisory cooperation is crucial to supervisory effectiveness in the Internet environment.

Of course, difficult issues may well be presented. For example, how much contact with a country must a foreign Internet institution have to warrant application of host country laws? And what legal sanctions might a home country have to vindicate its policies? These are far-reaching questions not covered by the EBG's work.

It's worth mentioning that efforts are underway to enlarge the realm of supervisory cooperation. Early last month, the Financial Stability Forum's Contact Group on E-Finance held its first formal meeting. This group, which I also chair, was formed to promote enhanced information-sharing among the various international sector-based working groups dealing with e-finance supervisory issues -- e-trading, retail payments systems, e-commerce, and so on.

At our recent meeting, we exchanged information on each other's work plans, took stock of e-finance developments, and explored areas for enhanced cooperation across industry sectors on supervisory policy. Three e-finance issues were identified as warranting consideration from a cross-sectoral standpoint: risk management principles for providing on-line financial services; greater prevalence of third party dependencies, including outsourcing; and cross-border issues. We agreed that while it would conduct no operational or policy development on its own, the Contact Group would serve as a clearinghouse for collaboration among the constituent working groups. Such collaboration, we believe, holds the key to effective supervision of e-finance activities in the future.

The future, members of the Contact Group agreed, is where the real challenges for supervisors lie. Because most e-finance activities are still in their infancy, the risks those activities present are not great at this time. What is urgent, however, is that we come to terms with the supervisory issues they present and build on the existing framework of international cooperation to address them. By understanding the issues and working together now, a practical cross-border approach to supervision should be attainable before the potential risks become a material reality.