NR 97-87
September 25, 1997

Remarks by Eugene A. Ludwig
Comptroller of the Currency

before the

Risk Management Planning Seminar
Washington, D.c.

September 25, 1997

Few people can better attest to the gap between the theory and practice of technology than the folks who man the customer support lines for the big personal computer makers. They've heard it all. According to a story in the Wall Street Journal, one technician reported taking a call from a woman who said she could not figure out why her new PC failed to respond to repeated pushes on the "foot pedal"-- her computer's mouse. Then there was the irate customer who complained that his fax modem wasn't working, even after he'd held the document up in front of the monitor and pressed the "send" button. And, the consensus favorite, the caller inquiring about warranty repairs on his computer's broken "cup holder" -- which, upon questioning, turned out to be the load drawer for the CD-ROM.

In a lighthearted way, these anecdotes remind us of something deadly serious: the costs and vulnerabilities associated with our ever-growing reliance on computer technology -- costs by no means limited to the feelings of helplessness and frustration that we all experience from time to time as we take part in the information revolution. Anyone whose data has been corrupted or obliterated by a computer virus or a hard drive crash -- anyone who has seen elaborate system security violated by a lone hacker knows that these problems are no laughing matter.

And neither is the problem I am here to speak to you about today: the year 2000. I trust that Steve Malphrus's presentation this morning cleared up many of your technical questions about Y2K. I propose to discuss the same subject from a somewhat different perspective.

When I first heard about the Year 2000 problem several years ago, I did not give it much thought. In those years I would have dismissed as alarmist suggestions that Y2K represented a serious potential threat to the safety and soundness of the banking system and to the global economy. To the extent that Y2K was a problem, it looked to me like a problem that the technical wizards who developed computers could easily handle.

That initial skepticism was misplaced. The Y2K problem is, if anything, more serious than we had imagined. We ought to be listening to the experts who hold seminars with titles like, "If You're Sleeping Soundly At Night, Then You Don't Understand the Year 2000 Problem." Because too many of us don't. Too many of us are still in denial. Too many of us continue to nourish

illusions that the solution is right around the corner. Or that the real impact of the problem will be limited to a handful of businesses particularly susceptible to it. Or that software vendors will take care of it. Or that we have plenty of time left to deal with it.

So I have two goals this afternoon. First, I want to disabuse you of any lingering misconceptions you may have on this score, and make it unmistakably clear that Year 2000 represents a challenge of major proportions that will not go away. Second, I want to tell you about the steps we are taking at the OCC -- both on our own and as a member of the U.S. and international bank regulatory communities -- to help protect against the possibility of serious harm to the world's financial structure when the clock strikes midnight on January 1, 2000.

Ultimately, however, the responsibility for averting catastrophe rests with you. The actions you take -- or do not take -- in response will determine the extent of the disruption that will occur on that momentous day. That there will be some disruption should by now be taken for granted. But by working together, we can minimize the pain and greet the coming millennium with optimism instead of anxiety.

One way of illustrating the seriousness of the problem is to hark back to a not nearly so momentous calendar anomaly -- February 29, 1996. That was a leap year day -- the day when the world got the first small hint of how calendar-related computer problems could disrupt the marketplace. This case involved just one stray day, as opposed to a millennium. The vast majority of the world's systems did not miss a beat. And yet . . . . The Brussels stock exchange had to shut down for the day, at a cost of more than $1 million in commissions. An aluminum factory in New Zealand likewise lost a day's production, worth another $1 million. The Arizona state lottery commission could not pay out winnings. Countless smaller events did not make the headlines but still involved significant losses for the firms involved. And this, remember, was an event involving a single day for which everyone thought they were prepared.

Time has become the enemy as we advance toward the millennium. For anyone who thinks otherwise, ask yourself when you last heard of the introduction of a new software application that did not require additional days or weeks or months beyond the original schedule. But the changes required to prepare for Year 2000 allow for no slippage. January 1, 2000 will wait for no one. The truth is that all the system changes will have to be in place at least a year before then, to allow the minimum time necessary for testing. Yet Y2K has been accurately described as "the project that cannot be late."

Indeed, some analysts say that it is already too late for those firms that have not already identified their needs and made provision for the technical assistance they need to implement and test the changes their systems require. I don't happen to agree with such fatalistic prognoses. But certainly the time is growing perilously short. In some relevant computer specialties,

the most talented technicians are already booked and committed to Year 2000 remediation. Any firm that has not yet developed a plan of action might pay a heavy price for procrastination. Depending upon their needs, they may find that help is unavailable at any price.

For banks, Y2K poses challenges of unprecedented urgency and complexity. Because the banking industry was among the first to adopt computer automation, banks today may well have more applications running simultaneously than any sector of the economy. Some big banks run thousands of applications, some superimposed on top of one another. Many have millions of lines of code, which have to be read to find which ones need modification. And then they have to be tested for interoperability -- not only with each other, but with the countless external systems, foreign and domestic, with which banks daily interact. Many experts tell us that the testing process will be the most difficult part of the whole process, because the fix adopted for one system may not be compatible with the fix adopted for another.

In addition, bankers have many things to worry about aside from getting their own houses in order. As you well know, today's world of financial services is intensely competitive. Bankers who are slow to solve the Y2K problem not only run operational risks, they invite predatory competitors who may be further along in the Y2K renovation process and will advertize that fact. We know, for example, that the securities trade association, the SIA, has moved aggressively to coordinate its members' response to the issue. The banking industry has no such coordinated effort under way. But let banks start missing interest payments, bungling stock transfers, or miscalculating dividend or maturity dates due to a Y2K slip up, and the world will hear about it from non-bank competitors. Bankers simply cannot afford to let that happen.

That's not the only external danger inherent in Y2K. When I say that the Year 2000 is a safety and soundness issue, I mean that in the most literal sense of the words. Many experts predict a rise in business bankruptcies among firms unable to complete timely Y2K renovations. I've seen estimates of business failures increasing by as much as 10 percent. Most businesses will feel the effects of Y2K project costs in their cash flows, which may impair their ability to manage and service debt. Banks can and must take steps now to minimize the risk that loans extended today will not turn sour on January 1, 2000. It is clear that they will have to be even more diligent about monitoring their customers' Y2K progress, in the same way that they now monitor their big customers' financial condition.

To help banks meet these challenges and the host of others related to the Year 2000, the OCC has undertaken a comprehensive plan of action, involving supervisory guidance, on-site inspection, and follow-up examinations or reviews. Our guidance has stressed two points: First, banks must implement a comprehensive project management program for their own computer processes, because correcting systems and software for the Year

2000 involves a broad sweep of a bank's operations. Contingency plans must be formulated to deal with unforeseen problems, and senior bank management should be directly involved in the entire effort. Second, banks need to account for the variety of potential risks attributable to the Year 2000, including reliance on vendors' renovation efforts, linkages to other systems, and potential credit risk exposure if large corporate borrowers fail to address their own Year 2000 problems.

These themes were embodied in the detailed statement issued in June 1996 by the federal banking agencies, working through the FFIEC -- a statement that strongly encouraged depository institutions to complete an inventory of core computer functions and to set priorities for compliance. In May 1997, the OCC and other agencies issued a second statement through the FFIEC, along with interagency guidance for banks and examiners on year 2000 project compliance. Still more detailed FFIEC guidance, suggesting practical solutions to some common problems, will soon be ready for issuance.

Because, as I noted earlier, Y2K is a problem with global ramifications, the OCC has taken the lead in focussing the attention of the international supervisory community on the issue. One thing that especially concerns us is that Y2K coincides with the scheduled introduction of the new European Currency Unit, the Euro. We want to make sure that, for institutions active in international currency trading, Y2K compliance does not suffer because scarce technical resources are being dedicated to Euro conversion instead. After extensive discussions and technical analysis, the G-10 Governors have just released a report that puts all Y2K issues into perspective, outlines the steps that financial institutions need to take to resolve the problem, and identifies the role of bank supervisors in helping to assure success. At the same time, the OCC has conducted a survey of large national banks to determine the extent to which Euro projects are interfering with Y2K compliance efforts. For the most part, bankers are telling us that they can manage both projects without compromising either.

Yet, as I told the Senate Subcommittee on Financial Services and Technology in testimony this past July, it is not enough that we issue advisories and leave it at that. The OCC has established a high profile on Y2K matters in the banks under its supervision. In conjunction with the interagency guidance released in May, we surveyed every national bank about its plans for dealing with Y2K.

Our survey found that some 85 percent of the largest national banks -- and a similar percentage of the large bank data processors and vendors -- had meaningful Y2K programs underway. For smaller banks, however, our survey produced more troubling results -- results recently confirmed by a Sheshunoff survey of state and national community banks. Fifteen percent of these banks have not taken the most basic steps in addressing this issue. Another 20 percent of these smaller banks are just starting to address the problem. Even among the larger banks, where the problem seems to be well understood, the steps being taken to meet it were often found to be inadequate. Weaknesses included a lack of a formalized budget dedicated to Y2K compliance, incomplete prioritization of

the systems to be corrected, and timetables not sufficiently aggressive to bring the bank into compliance in a timely manner.

We want all banks to succeed in meeting the Y2K challenge. We are doing everything in our power to ensure that banks under OCC supervision understand what the situation demands and respond accordingly. By the end of this week, I expect to release a letter to all national banks and vendor CEOs expressing my concerns about the banks that are not doing enough to prepare for the Year 2000. We will help in any appropriate way that we can. But let me emphasize that for banks that just don't get the message or take the necessary corrective steps, we will not hesitate to use any and all supervisory tools and enforcement powers to ensure that banks meet the safety and soundness challenge posed by the Year 2000.

The May FFIEC interagency statement and guidance informed banks that the federal banking agencies would be conducting uniform supervisory reviews of financial institutions' conversion efforts by mid-1998. Shortly thereafter, the OCC made the decision to examine, on-site, every national bank for Year 2000 compliance by that deadline. Since June, we have conducted nearly 250 of these examinations, with special attention to the community banks that our earlier survey identified as a problem area in regard to Y2K compliance. Although the results of this first round of examinations have not been fully analyzed, I can tell you that we are finding some problems that have to be dealt with. Community banks, which are much more likely to depend upon outside vendors for their data processing needs, also depend upon assurances from these vendors that they have the problem well in hand. In some cases, these assurances are entirely legitimate. In others, we find a great deal more wishful thinking than accomplished fact.

Let me make this absolutely clear: every bank must meet its timetable for compliance, whether data processing is performed in-house or by an external vendor. It is the bank's responsibility to monitor vendors' progress and to know their schedules for compliance. In the event that a vendor cannot meet established deadlines, the bank must exercise a contingency plan and secure those services elsewhere. The risks associated with non-compliance -- credit risk, operational risk, reputational risk, strategic risk -- will be borne by the bank, not the vendor.

This is one of those moments in time when we face a problem larger than any one of us alone. The responsibility upon each of us is great, and yet, as individuals, we can only do so much. Working in concert -- bankers, regulators, and vendors, in this country and abroad -- we can get the job done. Technology has long been our great strength. Let us work together to see to it that it does not become a serious stumbling block.

# # #

The OCC charters, regulates and supervises approximately 2,800 national banks
and 66 federal branches and agencies of foreign banks in the U.S., accounting

for more than half the nation's banking assets. Its mission is to ensure a
safe, sound and competitive national banking system that supports the citizens,
communities and economy of the United States.