TESTIMONY OF

EUGENE A. LUDWIG

COMPTROLLER OF THE CURRENCY

Before the

SUBCOMMITTEE ON FINANCIAL SERVICES AND TECHNOLOGY

of the

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

of the

UNITED STATES SENATE

July 30, 1997

Statement required by 12 U.S.C. □ 250:

The views expressed herein are those of the Office of the Comptroller of the Currency and do not necessarily represent the views of the President.

INTRODUCTION

Mr. Chairman, and members of the Subcommittee, thank you for conducting these important hearings and focusing public attention on the impact the year 2000 may have on American industry and the U.S. government. These hearings raise awareness of the issue, and help move businesses and the government toward solutions. Time is short -- there are only about 100 weekends remaining to complete any necessary computer recoding and testing -- and available technical experts in old computer languages are increasingly hard to find.

I also want to thank Chairman Bennett and Chairman D'Amato for your February letters to the banking agencies, which helped to focus our attention on the need to communicate more broadly about what we are doing to address the year 2000 problem in the banking industry. I welcome this opportunity to discuss the progress that national banks and the OCC are making in this area.

The OCC takes the year 2000 issue seriously, and we have an aggressive strategy to see that national banks are prepared, which includes an on-site examination of every bank under our supervision. My statement will describe the OCC's year 2000 program, which includes five major initiatives. First, the OCC and the other banking supervisors have worked hard to raise awareness within the industry of the full implications and the urgency of the year 2000 problem. In May, we issued joint guidance for depository institutions and examiners through the Federal Financial Institutions Examination Council (FFIEC). We plan to issue more detailed FFIEC guidance later this year, and it will stress the importance of testing and verification for establishing confidence in systems renovations.

Second, the OCC has reviewed every national bank and its vendors to assess plans for handling the year 2000 problem. This assessment revealed that, generally, the larger national banks and vendors have programs in place, but many smaller community banks are farther behind in their year 2000 efforts. Third, we are examining every national bank and its vendors on-site by mid-1998, with follow-up exams where necessary. Fourth, we are surveying the banks to find out whether they are considering the potential credit risk posed by large corporate borrowers who run into year 2000 problems; and also, whether they have encountered competing demands for their programming resources resulting from the scheduled 1999 startup of the Euro, the new European Monetary Union (EMU) currency. Fifth, we are in the midst of a comprehensive effort to prepare our own systems for the year 2000. The OCC is on schedule to complete, by September 30, 1998, all programming and testing changes necessary to ensure our systems are year 2000 compliant.

The OCC is committed to furthering a banking system that operates smoothly and efficiently as a financial intermediary. We recognize, however, that given the complex web of technologies used within banks, as well as the many other institutions with which banks exchange data electronically, malfunctions may still occur. Thus, our supervisory strategy is to prepare for the unexpected by having back-up strategies in place at the banks, and joint contingency plans ready to implement among the supervisory agencies. These efforts are of great importance to the public welfare. By making this issue a high priority for banks and for ourselves, we hope to minimize disruptions to bank operations and bank customers.

In the remainder of my statement, I will provide some background on banking's year 2000 problem. Then, I will discuss the five components of our program in greater detail.

The Year 2000 Problem

As we approach the 21st century, technology is an integral part of almost everything we do. The year 2000 problem has enormous reach, affecting almost every business, large and small. Communications systems, transportation services, and computers -- mainframes, networks and personal computers alike -- are all at

risk.

Modern conveniences and facilities, such as elevators, escalators, vaults, and alarm systems also may be affected. Computer programs for accounting, security, and bill payment need to be tested. All of these systems and processors will require some attention, to ensure that they will continue to operate at the turn of the millennium. And the more complex the reliance on technology, the greater the size of the task ahead of any given institution, private or public.

The core problem is technical in nature. Many computer systems will not recognize or process information with dates beyond December 31, 1999. The problem arises because, in an effort to be efficient with data storage (at a time when computer memory was at a premium), computer programmers often stored the year as two digits (97) instead of four (1997). When the next century arrives, computers may interpret the date "00" as "1900" and calculate inaccurate results when performing comparisons of dates, arithmetic operations, or sorting by date. Unless corrected, on January 1, 2000, computer systems worldwide may begin to fail or produce erroneous information.

There are two aspects to solving the year 2000 problem. First, users of technology must solve this problem with respect to their internal systems. That is, they must make sure that their internal computer systems properly handle date-dependent transactions and computations in the new millennium. Second, they must make sure that the systems they use can exchange date-dependent information effectively and efficiently with other, external systems. For many of the larger banks, solving the problem means reprogramming or upgrading in-house systems. For others, and for most of the smaller banks, reprogramming and upgrading must be done by the firms' data-processing services and software suppliers.

In all cases, addressing the year 2000 problem will require the rewriting of thousands of lines of code. There are two ways to manage this recoding, one permanent but costly, the other less costly, but temporary. The permanent solution is to recode all programs so they can read and write to a four-digit date format, but this process is also time-consuming and expensive. The other solution is to rewrite code so that low-value two-digit dates (e.g., 00, 01, 02...) are recognized as being years of the 21st century. This method would not be a permanent solution, but it would buy time in some situations as developers seek a more permanent solution, or as institutions wait to purchase new equipment in the future.

The task in front of businesses involves more than just selecting a solution or monitoring and testing a vendor's solution. Businesses need to think about the cost and timing required to replace computer systems or software, as opposed to repairing or upgrading them; the cost and availability of skilled personnel; the impact any considered merger or acquisition may have on meeting compliance deadlines; the compliance efforts of remote or overseas operations; the inclusion of compliance requirements in

any new vendor contracts and renegotiation of existing vendor contracts where possible; the bank's obligations to customers who rely on services and payments; and the date and calculation changes needed to account for the fact that the year 2000 is a leap year.

In addition to worrying about what might happen at the year 2000, computer servicers will have to figure out how to get past any disruptions that might occur in 1999 when the year field reads "99," and particularly, on September 9 of that year, when the date and year fields read "9/9/99." In what may be a preview of year 2000 computer responses, experts say that many computers will read these fields as a code for setting up special files or storing or kicking out the data processed, resulting in significant disruptions.

Banks and the Year 2000

The U.S. banking industry is particularly affected by the year 2000 problem because nearly every aspect of the business is dependent on computer systems for processing transactions and providing information. Technology is an integral part of the banks' interconnected information systems, where they exchange data daily with their customers, correspondents, vendors, other financial institutions, clearing houses, and corporate borrowers. Therefore, any malfunctions caused by the century date change could have an impact on a bank's ability to meet its obligations. Or, malfunctions could have an impact on the ability of others to meet their obligations to the bank. Some examples of bank systems where year 2000 problems may emerge include:

- Lending systems: To calculate interest payments, due dates, and past due amounts;
- Investment systems: To calculate accretions, amortization, and yields;
- Deposit systems: To calculate interest payments, overdrafts, and other fees;
- Accounting systems: To calculate accruals, depreciations; income and expenses;
- Fiduciary systems: To perform portfolio analysis, stock transfers; and calculate dividends and maturity dates;
- Management information systems: To integrate information by time period.

Solving the year 2000 problem will consume significant resources and demand the attention of bank management. Banks will spend considerable sums of money to fix the problem, particularly banks that do intensive in-house development of applications and databases. Many of the larger banks have thousands of programs, each with thousands of lines of code. And smaller banks will face substantial resource and attention demands because vendors' conversion efforts are often expensive and difficult to verify.

In addition, the year 2000 project will divert resources and attention away from other business activities that might add new

value to the bank. Yet banks cannot afford to do the job poorly, because of the inconvenience customers are likely to experience and the resulting damage to banks' reputations and market share.

The year 2000 problem also brings new legal risks to the banks because of their fiduciary or contractual responsibility to customers and associates. In the event that the computer systems upon which banks rely do not have the capability to handle processing of transactions in the new millennium, and/or these systems produce erroneous information, there is the potential for bank liability.

These issues characterize the year 2000 problem in the financial services industry and dictate many aspects of the OCC's supervisory response, which I will now describe.

OCC SUPERVISORY STRATEGY

As chairman of the FFIEC -- whose membership includes representatives of the Federal Reserve, the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration, the Office of Thrift Supervision, and the OCC -- I am working aggressively with the other banking agencies to make this issue a priority with bankers and their vendors and service providers. The banking agencies first alerted the financial services industry to our concern over the year 2000 problem in a June 1996 FFIEC statement. In that statement, we strongly encouraged depository institutions to complete an inventory of core computer functions and to set priorities for compliance changes, keeping in mind that testing should be underway for mission-critical systems by December 31, 1998. In May of this year, the OCC and other agencies issued a second statement through the FFIEC, together with interagency guidance for banks and examiners on year 2000 project management.

And our next issuance of FFIEC guidance, which I mentioned earlier, will be more detailed and suggest some practical solutions to common problems. It will emphasize the importance of verification and testing cycles and timetables. The initial FFIEC guidance emphasized two important points that are essential to addressing this problem. One, banks need to address several external sources of potential risk attributable to the year 2000 problem, which I will explain next. Two, banks must implement a comprehensive project management process, because correcting systems and software for the year 2000 involves a broad sweep of a bank's operations.

External Risks

Fixing internal computer systems alone will not take care of year 2000 exposure. Bank systems interact every day with other computers, and each of these electronic relationships poses a potential risk to the bank. The three primary external risk areas are:

Reliance on Vendors -- The heavy use by banks of vendors for performing critical operational processes, such as deposit

posting or check sorting, requires that banks closely monitor their vendors' conversion programs and determine if contract terms can be revised to include year 2000 covenants. Banks must have alternative service and software providers identified in the event that vendors cannot correct their systems or software adequately or quickly.

Data Exchange -- The multiple linkages banks have with other parties -- other financial institutions, governments, borrowers, and depositors -- require that banks allow sufficient time to assess the effects of their year 2000 solutions on data transfers and exchanges. These linkages are especially apparent in the interrelationship among payment systems at the local, national, and international levels. Banks must be able to exchange payment information to clear checks, process electronic transfers, and maintain data for customers. Larger banks may have additional responsibility to process payrolls or pension payments for smaller institutions and customers.

The international dimensions of the year 2000 problem are a serious concern to bank regulators because of these interconnections. Domestically and across borders, banks, payment systems, and government agencies must be able to handle year 2000 processing and communicate with each other to facilitate normal banking and commerce. The OCC, together with the Federal Reserve and the FDIC, is working closely with the Basle Bank Supervisors Committee to reach international agreements on year 2000 solutions. We pressed hard to advance this issue and to obtain a committee report for supervisors, which is to be released in September. These efforts and others help raise awareness around the world of the need to address the year 2000 problem.

Corporate Customers -- Banks need to consider in their assessments of credit risk whether a prospective borrower might experience cash flow or other problems due to his or her own year 2000 problems. Consequently, as part of our year 2000 program, we are telling banks to evaluate the compliance efforts of their own customers and to factor this information into their loan underwriting.

Year 2000 Project Management Process

A comprehensive and effective year 2000 project management process is crucial. We expect this management process to be specific and formally drafted for financial institutions with complex systems or institutions that write much of their own computer programs. All financial institutions, regardless of size or complexity, will require strong leadership, effective communication, and accountability to ensure that year 2000 initiatives will be successful. Our guidance enumerates the five phases necessary to properly manage a computer conversion program: awareness, assessment, renovation, validation, and implementation.

Awareness Phase -- During this phase, management needs to become educated about the year problem at its institution and to

establish executive level support for the resources necessary to correct the problem. This phase is also when management puts together a year 2000 program team to begin the development of an overall strategy that encompasses in-house systems, servicers for systems that are outsourced, and vendors, auditors, customers, and suppliers, including correspondent banks. Banks should have already passed this stage.

Assessment Phase -- This phase includes identifying all hardware, software, networks, automated teller machines, other various processing platforms, and customer and vendor interdependencies affected by the year 2000 date change in order to assess the size and complexity of the problem. The assessment should go beyond information systems and include environmental systems that are dependent on microchips or software, such as security systems, elevators, and vaults. Management also needs to evaluate year 2000 effects on other strategic business initiatives.

During this phase, project managers must identify resource needs and establish the schedule and the sequencing of the year 2000 project. Resources needed include appropriately skilled personnel, contractors, vendor support, budget allocations, and hardware capacity. This phase is when management clearly identifies corporate accountability throughout the project, and sets policies to define reporting, monitoring, and notification requirements. Finally, contingency plans must be developed to cover unforeseen obstacles during the renovation and validation phases and must include plans to deal with lower priority systems that would be fixed later in the renovation phase. This phase should be completed by the third quarter of 1997.

Renovation Phase -- This phase includes code enhancements, hardware and software upgrades, system replacements, vendor and other associated changes. Information gathered during the assessment phase should be used to prioritize the work program. For institutions relying on outside servicers or third-party software providers, ongoing discussions with the vendors and monitoring their progress are necessary. Backup data processors are lined up as part of contingency planning.

Validation Phase -- Testing is critical to a year 2000 project and plays a major role in the last three phases of the project management plan. Only through testing can year 2000 compliance be verified, and new testing must be performed with every incremental change to hardware and software components. This phase includes verifying connections with other systems and verifying the acceptance of all changes by internal and external users. Management should establish controls to assure the effective and timely completion of all hardware and software testing prior to final implementation. As with the renovation phase, financial institutions must be involved in ongoing discussions with their vendors on the success of their validation efforts. This phase needs to be completed, with testing fully underway by December 31, 1998.

Implementation Phase -- This phase includes making sure that

systems are year 2000 compliant and acceptable to business users. For any system that is unacceptable, the business effect needs to be assessed clearly and the organization's year 2000 contingency plans must be implemented. Project managers must bring any potentially noncompliant mission-critical system to the attention of executive management immediately for resolution. In addition, during this phase, management must make absolutely sure that any new systems or subsequent changes to verified systems are compliant with year 2000 requirements.

SUPERVISORY ACTIONS

As I have noted, the OCC is actively engaged with the other banking agencies, through the FFIEC, in supervisory planning to address the foregoing concerns about year 2000 project management and risk management issues. The OCC also is taking special steps to target year 2000-related issues of particular concern to national banks and examiners.

Interagency Working Group: The member agencies of the FFIEC are working together to promote uniformity in year 2000 supervision across depository institutions and to combine forces when tackling shared problems. We have formed an interagency working group to handle a number of year 2000-related issues, such as coordinating supervisory activities for vendors; educating and lecturing on year 2000 issues through trade groups and public events; and drafting contingency planning and training programs for quick and effective supervisory responses where needed. An interagency group of examiners and legal representatives will analyze different scenarios to design effective, joint, rapid response techniques for regulators.

Readiness Assessments: In conjunction with the release of interagency guidance in May, the OCC initiated a first round of assessments of every financial institution we supervise in order to gauge the institution's readiness for the task ahead. This general assessment helps us identify which banks are the least prepared for the year 2000. These institutions will then receive priority attention. The OCC surveyed each banking company and found that about 85 percent of large banks -- controlling about the same percentage of national bank assets -- have programs in place. We found a similar level of preparedness among large bank data processors and vendors.

This survey does not tell us whether these programs will get the job done; that will only begin to become clear when testing is fully underway. However, it does identify several common weaknesses in large bank program management, including a lack of a formalized budget, incomplete prioritization of systems to be corrected, and timetables that are not sufficiently aggressive to bring the bank into compliance by our December 31, 1998 deadline. We are working first with those banks that appear unlikely to meet the compliance deadline, requiring them to move more swiftly to supply the necessary funding and personnel to get the job done.

Our survey also shows that a number of the community banks --

holding the remaining 16 percent of national bank assets -- need to step up their efforts. We found that about 15 percent of these smaller banks are not aware of the effect that the year 2000 will have on their businesses. Another 20 percent, though aware, are just starting to address the issue. The slower reaction to the year 2000 problem by the smaller institutions relative to larger ones reflects the smaller banks' greater reliance on vendors for processing and software needs. But the banks must meet the same supervisory timetables, whether data processing is in-house or provided elsewhere, and banks using vendors need to monitor vendors' progress and know their schedules for compliance. We are working very closely with the banks to make sure they understand what is expected of them, and we anticipate that they will make a responsible effort to meet our supervisory expectations. However, the OCC will not hesitate to use its supervisory tools and enforcement powers to compel banks to take appropriate action.

The OCC has recently completed two additional year 2000-related surveys. The first indicates to what degree large national banks are considering the year 2000 exposure of their major corporate borrowers. The second survey considers the drain on bank resources of preparing for the new Euro, which may compete for resources with year 2000 compliance efforts.

Year 2000 Exposure of Large Corporate Borrowers: The value of bank loan portfolios may be affected if borrowers are unable to meet their payment obligations to the banks because of the borrowers' own year 2000 malfunctions. For this reason, the OCC has surveyed the largest national banks to find out if they have considered the credit risk their largest corporate borrowers may pose. The assessment looked at the 24 largest national banks that pool their resources to make the largest corporate loans, which start at $25 million. The banks surveyed underwrote approximately $434 billion in syndicated loans in 1996, representing 80 percent of the syndicated loans originated by national banks and 36 percent of all outstanding syndicated loans.

Our results show that while large national banks are aware of the credit implications of the year 2000, most need to take additional actions to address the issue with current or potential borrowers. Nonetheless, most banks surveyed are in the process of determining what should be done to address year 2000 credit risks. More than half will review year 2000 plans with corporate borrowers, and one-third plan to include year 2000 analyses in their file documentation or credit review process. The OCC plans to address these credit risk issues in future industry and examiner guidance, in order to ensure that examiners verify that a bank incorporates a borrower's year 2000 preparations into its underwriting standards.

European Monetary Union: The OCC has surveyed the handful of national banks, federal branches, and data centers active in foreign currency transactions to find out whether the scheduled 1999 introduction of the new Euro currency may place significant competing demands on scarce technical resources. None of the

institutions surveyed said that their EMU projects pose conflicts for their year 2000 projects. We will continue to monitor this issue.

Bank Examinations: The May FFIEC interagency statement and guidance informs banks that the federal banking agencies will be conducting uniform supervisory reviews of financial institutions' conversion efforts by mid-1998. The OCC made the decision to examine, on-site, every national bank for year 2000 compliance by that deadline, and we now have these examinations underway. In notifying the banks about these year 2000 examinations, the OCC emphasized that it would look for comprehensive planning and a clear commitment to meeting year 2000 goals. We informed the banks that special attention would be focused on whether senior management and the board of directors are fully engaged in the planning and monitoring of year 2000 conversion efforts.

Following these examinations, the OCC will undertake appropriate follow-up activities to ensure that banks address identified problem areas and also to assess the effectiveness of the institutions' testing programs. If we find that a bank is encountering significant problems, our examiners will work with bank management to see that it corrects problems in the most critical systems. As indicated by our readiness assessment, small institutions, in particular, may need added attention from examiners. In addition, we are establishing a formal reporting process to monitor trends and identify issues quickly that arise out of our year 2000 examinations. This process includes an ongoing dialogue between agency staff in Washington and in the field to ensure that policies are implemented consistently. Any bank that falls behind in meeting crucial compliance deadlines will face the same kinds of supervisory actions that are brought on by other safety and soundness concerns.

Vendor Examinations: As I noted previously, focusing on the activities of financial institutions alone will not prevent year 2000 disruptions in the banking industry. Banks rely heavily on vendors and servicers. Therefore, the OCC and the other banking agencies will conduct joint examinations of nonbank data-processing centers and software companies before mid-1998, using our supervisory authority provided by the Bank Service Company Act of 1962. As part of our initial assessment of the banks, we compiled a list of all the vendors used by each national bank. This list will enable us to alert those banks that are using a particular vendor who is found to have significant year 2000 problems.

OCC's Internal Efforts to Address The Year 2000 Problem

In May of last year, just prior to sending our first advisory to the banks, the OCC implemented its own program to address the year 2000 transition. However, we have been aware of the issue for quite some time, and have been following a four-digit year standard in all development efforts since 1991. Even so, the agency is facing the same conversion difficulties, system upgrade expenses, and testing frustrations as every other business operation. All platforms, hardware and software must be verified

as year 2000 compliant. Purchased software must be tested for compliance in our data-sharing environment. We expect the most challenging coordination efforts to be found in time-sensitive testing and in putting systems back into production.

Some of the things we are doing now include:

- mission-critical systems have been identified and prioritized;
- less critical systems have also been scheduled for conversion/testing;
- we are monitoring vendors and including compliance requirements in contracts;
- we have developed a testing strategy and a test plan template;
- we have identified an overall contingency plan strategy for each mission-critical system; and,
- we are communicating with our data exchange partners.

Our senior managers are aware of the Year 2000 problem and involved in the project. The OCC Executive Committee has budgeted $1.1 million this year for information systems changes underway now. Next year, the Executive Committee considers additional funding for infrastructure systems changes, such as the purchase of a new building entry system. A project team of OCC employees is assigned to this task, each of whom is responsible for efforts in the areas of finance, procurement, supplies, and building services departments. We are currently on schedule to complete all compliance programming and testing by September 30, 1998.

CONCLUSIONS

As Comptroller, I have a responsibility to do all I can to ensure the National Banking System and the OCC is prepared for the Year 2000. We have an aggressive program in place to ensure that national banks are prepared. This program includes an explicit project-management timetable:

- National banks must identify mission-critical applications and set priorities for year 2000 tasks by the end of the third quarter 1997. Most financial institutions and service providers are already well into this phase of the project;
- Our examinations of bank and vendor preparations will be completed by June 1998;
- Banks must largely complete code enhancements and revisions, hardware upgrades, and other changes that follow the assessment phase by December 31, 1998;
- Testing for mission-critical systems must take place throughout the compliance effort, but be fully underway no later than January 1, 1999.

In my role as chairman of the FFIEC, I have worked with the other banking agencies to provide uniformity among our supervisory actions, and put financial institutions largely on the same schedule, which may help them coordinate their testing and verification cycles. In the international arena, the OCC and the

other supervisory agencies have pressed for cross-border understanding of the need to provide similar uniformity and coordination among countries.

It is important to keep in mind that the transition to the Year 2000 will pose the greatest challenges to banks and vendors that perform their own programming. Hence, they need to be particularly vigilant about testing and re-testing their systems. Furthermore, testing is quite a complex matter. Banks must test all their computer systems to make sure they can process dates after the year 2000, and then test them again to make sure that the method used to process dates is compatible with the methods used by the customers and correspondents with whom a bank exchanges data and funds. This requires that banks work closely with their customers and correspondents -- whether they be other financial institutions, vendors, government agencies, or foreign entities -- to coordinate a smooth transition to year 2000 compliant electronic-transfer interconnections.

Nonetheless, even with these many precautions, year 2000 malfunctions are likely to occur because of the banking industry's reliance on technology and its complex relationships with other businesses. Through our extensive efforts to prepare for this event, the work of our fellow regulators, and the efforts of the banks, we hope to minimize any disruptions to banks and their customers.