For Release Upon Delivery
November 4, 1997, 2:00 p.m.

TESTIMONY OF

EUGENE A. LUDWIG

COMPTROLLER OF THE CURRENCY

Before the

COMMITTEE ON BANKING AND FINANCIAL SERVICES

of the

U. S. HOUSE OF REPRESENTATIVES

November 4, 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 Committee, thank you for conducting this important hearing and focusing public attention on the impact the year 2000 problem may have on the banking industry and the U.S. government. Achieving awareness in business, government, and the public is the critical first step towards obtaining year 2000 compliance. Given the complexity of the task, we must move aggressively. The attention the Congress is devoting to the year 2000 challenge is timely and underscores the importance of the issue.

The year 2000 problem poses a difficult and wide-ranging challenge to the banking industry and the American economy. All users of communications, computer, or office automation technology face year 2000 risks and must prepare for the century date change. They must maintain the integrity of their internal systems and address external risks associated with connecting to other systems. The banking industry's readiness is especially important, because banks are at the center of our payments system and credit flows in the economy. Any operational and systems malfunctions caused by the century date change could have an impact on a bank's ability to meet its obligations. Of equal concern are malfunctions that bank customers may experience that could prevent them from meeting their obligations to the bank. These problems, if not addressed, could have repercussions throughout the nation's economy. Adding to the challenge is the difficulty in finding sufficient programmers who are familiar with old mainframe languages.

Larger banks, which hold the majority of the industry's assets, frequently have computer applications that were developed in-house. These banks must examine their systems carefully to determine the changes necessary to make them year 2000 compliant and effect those changes. Many smaller banks rely heavily on vendors for data-processing and software services as a more cost-effective way to manage their operations. Banks that depend on vendors to achieve year 2000 compliance must carefully manage their relationships with such vendors and service providers, making sure that these vendors commit the necessary time and resources to make their products year 2000 compliant.

Given the complex web of technologies financial institutions use, as well as the many other institutions with which they exchange information electronically, no one can guarantee that no problems will occur when the clock strikes midnight on December 31, 1999. Malfunctions may occur. But the Federal Financial Institutions Examination Council (FFIEC), which I currently chair, and the federal bank and thrift regulatory agencies individually are taking vigorous steps to protect against the possibility of serious harm to the nation's financial system.

Since last year, the regulatory agencies have undertaken a number of initiatives in preparation for the year 2000. Our supervisory strategy is aggressive and comprehensive. It involves alerting financial institutions to the nature of the problem; assessing the risk at each

institution by conducting careful examinations; requiring institutions to address the problem and monitoring their progress; preparing for the unexpected by ensuring that institutions have back-up strategies in place; and developing joint contingency plans among the supervisory agencies. The success of those actions will have an important impact on the public welfare. By making these actions a top priority for depository institutions and their supervisors, we hope to minimize disruptions to bank operations and to bank customers.

As requested in your letter of invitation, my statement today will address the year 2000 problem and its implications for the safety and soundness of the nation's financial system. As part of this discussion, you asked that I discuss the associated insurance, legal, and security issues. Then, I will highlight the FFIEC's initiatives and the Office of the Comptroller of the Currency's (OCC) implementation of those actions. I will specifically address your questions regarding the importance given to year 2000 preparedness when assigning CAMELS ratings, the contingency planning that is necessary to prepare for problems that may arise despite the best preparation on the part of financial institutions (with a particular focus on liquidity), and the preparedness of the international banking community.

To begin, I will discuss the year 2000 problem in more detail.

THE YEAR 2000 PROBLEM

Information technology is an integral part of almost everything we do. Accordingly, 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 greater the reliance on technology, the greater the size and complexity of the task ahead for any institution, private or public.

The year 2000 problem arises because many information technology systems currently in use will not recognize or process information with dates beyond December 31, 1999[1]. The problem results from efforts to store data efficiently in the early years of computer development, when computer memory was at a premium. In those years, computer programmers made the decision, almost universally followed, to store the year as a two-digit

[1]Computer systems may begin to experience problems well in advance of the year 2000, when making calculations or triggering dating mechanisms that look at or beyond the year 2000. For instance, an application that schedules events 12 months in the future, may begin to experience problems on 1/1/1999, a full year in advance of 2000.

number (e.g., 75) instead of a four-digit number (e.g., 1975). Therefore, when the next century arrives, computers may interpret the date "00" as "1900" and thus produce inaccurate calculations when performing comparisons of dates, arithmetic operations, or sorting by date. Indeed, unless corrected by January 1, 2000, information systems worldwide may not only produce erroneous information, but in many cases may fail altogether.

Newer computer systems may be year 2000 compliant; however, many older systems and applications must be modified[2]. For larger institutions, this can mean reviewing millions of lines of code to identify those that need modification and making the necessary corrections. There are several ways to manage this recoding. Some options are permanent but costly. Others are less costly but temporary. One permanent solution is to recode all programs to read and write to a four-digit date format, but this process is also time-consuming and expensive. Another 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 to put in place a permanent solution.

Addressing the year 2000 problem involves more than just selecting a solution or monitoring and testing a vendor's solution. Businesses need to think about a variety of issues, including, importantly: 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 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.

Impact on the Banking Industry

Banking is one of the most information-intensive businesses in the American economy. As such, it has historically been exceedingly reliant on information processing technology and was, in fact, an early adopter of many of the systems and applications that now need to be fixed. Today, nearly every aspect of the banking industry is dependent on computer systems for processing transactions and providing information. Banks exchange data daily with their customers, correspondents, vendors, other financial institutions, clearing houses, and corporate borrowers. Thus, financial institution applications must be not only revised or replaced to become year 2000 compliant, but, as noted above, they must also be tested for interoperability with the numerous internal and external systems -- foreign and domestic -- with which banks

[2]Not all hardware or software systems manufactured in the last few years are necessarily year 2000 compliant as many new products still rely on older technology. Banks should check with their vendors or software publishers to determine if their applications and hardware are year 2000 compliant. Key software and hardware that interact with mission critical applications should be included in the overall year 2000 testing program.

interact. Many experts tell us that the testing process will be the most difficult and time consuming challenge, because the fix adopted for one system may not be compatible with the fix adopted for another.

Solving the year 2000 problem will take significant resources and demand the attention of bank management. Banks will spend considerable sums of money to prepare, particularly larger banks, which generally do intensive in-house development of applications and databases. Smaller banks will face substantial demands on their resources because vendors' conversion efforts are often expensive and difficult to verify prior to installation.

In your invitation letter, you asked us to discuss specific legal, insurance, and security issues related to the year 2000 problem. Many of these issues are complex and multi-faceted. We believe that, as banks move forward in addressing the year 2000 problem, more of these issues are likely to emerge.

Legal and Insurance Issues. There are two categories of legal and insurance issues arising from potential year 2000 problems: first, who should pay for correcting a bank's year 2000 problems; and second, if the year 2000 problems are not corrected, who should bear the liability resulting from the failure of any bank's systems?

As was previously noted, the cost of correcting a year 2000 problem can be great. A bank's legal right to correction or replacement by a supplier of computer services, software, or equipment that are not year 2000 compliant is largely controlled by the contract between the bank and the vendor. However, the terms of these contracts vary considerably and banks will need to review them to determine general warranties or express provisions that might apply to year 2000 compliance.

If undetected or uncorrected year 2000 problems cause a bank's systems to fail, the bank could breach many legal obligations arising from its fiduciary and contractual relationships with customers. For example, the bank might no longer be able to comply with its contractual obligation to depositors to keep accurate records on account balances or to make timely payments in accordance with the instructions of demand account customers. The bank's systems might also improperly refuse debit, credit or ATM cards. Indeed, this has already happened. Late last year, one bank discovered that credit cards it had issued with expiration dates beyond 1999 were not being honored by point of sale terminals because its credit card processing software was not year 2000 compliant[3]. As these examples illustrate, a bank's extensive contractual relations with retail and wholesale customers and the intrusive nature of

[3]Jeremy Quittner, "As Year 2000 Looms, Issuers Play Beat the Clock," The American Banker, August 5, 1997.

the year 2000 problem could result in failure to perform on many obligations giving rise to extensive liabilities.

Banks facing liability for year 2000 problems may have means to shift or reduce that liability. Banks need to review vendor and servicer contracts to evaluate their rights in this regard. However, banks should not assume that this route is a cure to their problems. For example, many equipment and software purchase and license contracts limit the liability of the provider to the cost of the equipment or software.

Banks and bank vendors also may have insurance policies that cover their liability due to a year 2000 problem. Whether and the extent to which a particular bank is covered depends, of course, upon the contractual language in the relevant insurance policy. Again, banks will need to review their insurance policies to determine if coverage might extend to the costs or liabilities arising from year 2000 problems. For example, some believe that business interruption polices will not cover losses due to year 2000 system failures because year 2000 problems are not "fortuitous" events covered by those policies[4].

Further, a bank selecting a firm to correct its year 2000 problems will have to consider whether the firm's insurance policy would cover liability for the bank's failure to perform. Similarly, the bank might well wish to seek contractual assurance that the selected firm will indemnify the bank for any losses arising from year 2000 problems it contracted to fix.

Some insurance companies are apparently offering policies specifically covering year 2000 risks, including unforseen business disruptions. Generally, these policies have limitations of between $100 million and $200 million, and the companies offering such policies have indicated that they will be selective as to which firms they insure[5]. For example, some require that applicants document their year 2000 plans and require that an accounting firm review those plans before the application is accepted. The coverage is also expensive. It is reported that, in many cases, the insured party is expected to pay from 50 percent to 85 percent of the risk limit during the period of coverage. In some cases, however, 90 percent of the premium will be returned if the insured institution experiences no year 2000 problems[6]. Bank management will have to evaluate their specific situation to decide whether the purchase of such insurance is justified. In any event, the purchase of insurance is not a substitute for reasonable and prompt measures to ensure that the bank and its counterparties are year 2000 compliant.

---

[4]Jinnett, supra and David Schaffer, "Insurance and Y2K," February 1997.

[5]Thomas Hoffman, "CIOs wary of year 2000 insurance," Computerworld, February 3, 1997; Jinnett, supra.

[6]Hoffman, supra; Charles Holt, "Glitch Guard," Kansas City Business Journal, September 29, 1997.

Security. The year 2000 problem also highlights a security issue of growing concern to supervisors. Banks increasingly will rely on consultants and vendors to solve their myriad information technology problems, including the need to bring their systems into compliance for the year 2000. It is important that banks assure themselves that they know their service providers and are confident that those parties will not compromise banks' information security. This means: a) monitoring third parties to prevent security breaches, and b) requiring vendor contracts to have a confidentiality provision. Just as bank supervisors have told bankers to "know their customer," banks must also "know their vendor."

I would now like to discuss the initiatives the FFIEC is undertaking to address these issues.

FFIEC INITIATIVES

The issues outlined above will have a profound impact on the banking industry if institutions do not effect timely remedial action. As the current chairman of the FFIEC, I am committed -- as are the other financial institution regulatory agencies -- to pursuing a forceful agenda to ensure that insured depository institutions address year 2000 issues in an aggressive manner. One part of this agenda is a series of initiatives designed to inform financial institutions of systemic issues and outline regulatory expectations as we oversee their year 2000 project efforts.

The FFIEC first alerted the financial services industry to our concern over the year 2000 problem in a June 1996 statement. In that statement, the FFIEC member agencies strongly encouraged depository institutions to complete an inventory of core computer functions and have reprogramming efforts complete by December 31, 1998. In May of this year, the FFIEC issued a second statement, which included interagency guidance for depository institutions and examiners on year 2000 project management.

The May guidance emphasized two important points that are essential to addressing the year 2000 problem. First, depository institutions need to address external sources of potential risk attributable to the year 2000, in addition to their internal sources of such risk. Second, depository institutions must implement a comprehensive project management process to address these risks, because correcting systems and software for the year 2000 involves a broad sweep of an institution's operations. I will elaborate on both of these points.

External Risks

In-house fixes to internal computer systems will not solve an institution's year 2000 problems. Most depository institutions rely on third party vendors for some data processing

needs. Moreover, their systems interact daily with other computer systems, and each of these electronic relationships poses a potential risk to the depository institution.

Reliance on Vendors. Depository institutions' reliance on vendors for performing critical operational processes, such as deposit posting or check sorting, requires that the institutions closely monitor their vendors' conversion programs and determine if contract terms can be revised to include year 2000 covenants. Depository institutions must have contingency plans identifying alternative service and software providers in the event that vendors cannot correct their systems or software adequately or quickly.

The FFIEC will hold a vendor conference on November 10. It will provide a forum for vendors, depository institutions, and their supervisors to express their concerns and clarify regulatory expectations. We will be shortly issuing FFIEC guidance for depository institutions on the vendor management due diligence process. This guidance will emphasize the key components of any vendor management process: the financial institution should know whether its vendor has the financial capacity to make necessary changes; the financial institution should establish appropriate contingency plans, with trigger dates, to allow plenty of time to change course and use different service providers; the financial institution should identify its contractual rights and responsibilities, as well as those of its vendors; the financial institution should establish an ongoing system of communication with service and software providers; and the financial institution should develop a plan detailing how and when it and its vendors will test the interoperability of system or software changes.

Clearly, the reliability of vendor-provided products and services will be critical to the success of many financial institutions' efforts to address the year 2000 problem. Because a vendor's customers could include banks, thrifts, and credit unions, the regulatory agencies will conduct joint examinations of nonbank data-processing centers before June 30, 1998, using supervisory authority provided by the Bank Service Company Act. The FFIEC intends to accelerate the examinations of the largest data processing centers and companies that publish depository institution software so that this important information may be gathered as soon as possible. We are also implementing a quarterly monitoring program for all major vendors, which will track vendor progress in executing their project plan.

Data Exchange. The multiple linkages banks have with other counterparties -- other financial institutions, governments, borrowers, and depositors -- require that financial institutions allow sufficient time to assess the effects of their year 2000 solutions on data transfers and exchanges. It is not enough for insured depository institutions just to make their systems year 2000 compliant. Should their counterparties fail to address the year 2000 problem, or adopt a method which produces data that are unrecognizable by the financial institution, electronic fund transfers might fail or financial institution systems might be contaminated with corrupt data.

To manage these challenges, financial institutions will have to institute a comprehensive process which tests the linkage with each counterparty. The number of linkages that need to be tested can grow geometrically due to the interrelationships among payment systems at the local, national and international levels. Consequently, much of our focus as regulators in 1998 and beyond must be directed at ensuring that financial institutions' year 2000 project management plans include comprehensive testing programs. The Federal Reserve Board will play a very significant role in coordinating the year 2000 testing process, because of their payments system responsibilities The FFIEC intends to provide further guidance outlining regulatory expectations for testing in early 1998.

Relationship with Counterparties. Insured depository institutions must ascertain how well their counterparties, who also rely on computer systems, are addressing the year 2000 problem. Counterparties that do not address these problems may experience operational or financial problems that may make it difficult for them to conduct business. If loan customers or bond issuers cannot repay their debt as agreed, the financial institution faces increased credit risks. If derivative counterparties cannot settle maturing transactions, the financial institution potentially faces not only increased transactional risk, but also increased credit risk, depending on the net position of the contract. If fund providers cannot deposit or maintain funding agreements, the financial institution faces potentially increased liquidity risk. The FFIEC's May Interagency Statement outlined the due diligence process that banks should undertake in assessing the year 2000's potential impact on their credit exposure. We are developing guidance that extends the due diligence process to all the key counterparties of a financial institution.

Year 2000 Project Management Process

The second major focus of the May FFIEC guidance was to outline a comprehensive and effective year 2000 project management process. This management process begins with a written statement that focusses on the specific issues arising at each insured depository institution. But that is not enough. All financial institutions, regardless of size or complexity, will require strong leadership, effective internal and external communication processes, and clear lines of accountability to ensure that year 2000 initiatives will be successful. The FFIEC guidance enumerates the five phases or stages 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 2000 problem at its institution and establish executive level support for the resources necessary to correct it.

Assessment Stage. This stage of the process includes identifying all hardware, software, networks (including those dealing with security systems, elevators, and vaults),

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. During this period, project managers must identify resource needs and establish the schedule and the sequencing of steps in the year 2000 project. Resources needed include appropriately skilled personnel, contractors, vendor support, budget allocations, and hardware capacity. As well, the financial institutions must also develop contingency plans. Most financial institutions should have completed these stages by now.

Renovation Phase. This phase includes code enhancements, hardware and software upgrades, system replacements, vendor and other associated changes. Institutions relying on outside servicers or third-party software providers must hold ongoing discussions with the vendors and monitor their progress. Backup data processors should also be lined up as part of contingency planning. This phase needs to be completed, with testing fully underway for mission critical applications, by December 31, 1998.

Validation Stage. Testing is critical to a year 2000 project and plays a major role in the final stages of the project management plan. Only through a comprehensive testing program can year 2000 compliance be verified. This stage 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.

Implementation Phase. During this phase, management must verify that systems are year 2000 compliant and acceptable to business users. For any system that is unacceptable, financial institutions must clearly assess the business effect of that system and implement the organization's year 2000 contingency plans.

Upcoming Activities

As they observe the work depository institutions have underway to fix their systems and programs, regulators have identified several problems shared by many of these institutions. The FFIEC member agencies are working on joint guidance that addresses and suggests some practical solutions to these common problems.

Guidance. The FFIEC has four planned issuances of guidance that will address: 1) enterprise risk; 2) counterparty issues; 3) vendor management; and 4) testing. The issuance on year 2000 business enterprise risk will provide guidance to bank boards of directors on ensuring that senior management is addressing the effects of the year 2000 problem on their business. The counterparty guidance will set forth the minimum due diligence process we

expect financial institutions to follow in assessing how the year 2000 affects their large clients. The vendor management guidance, which I discussed earlier, will outline the due diligence process that financial institutions who rely on vendors should follow in analyzing their vendors' ability to address the year 2000 problem. The testing guidance (also mentioned earlier) will review testing issues and clarify what all financial institutions, large and small, should do to ensure their systems are year 2000 compliant. The FFIEC will issue further year 2000 guidance throughout 1998 and probably into 1999, as other issues and concerns are identified.

Outreach and Contingency Planning. It is important for the FFIEC member agencies to have ongoing discussions of year 2000 issues with financial institution managers and industry trade associations. By working together, we can best ensure that the industry is well-positioned to solve the problems posed by the year 2000. To that end, the FFIEC member agencies have formed a working group comprised of supervisory, legal, and receivership experts to review a number of questions, including coordinating vendor examinations. In May, the working group met with six of the larger banking trade groups to discuss further steps we could be taking to increase industry awareness. It plans to hold another joint meeting later this year.

With respect to our contingency planning, we are determining what steps regulators must take to handle problems that may arise in critical systems. The Federal Reserve Board is focussing on potential disruptions to the payments system, while the Federal Deposit Insurance Corporation is looking into liquidation and resolution matters. The OCC is working to ensure its examiners are prepared to address year 2000 problem situations quickly and consistently across the national banking system.

The forthcoming FFIEC guidance will make clear that it is important that financial institutions monitor their vendors' progress. In the event that a vendor cannot meet the FFIEC's schedule, the financial institution needs to take steps to secure services elsewhere. The risks associated with non-compliance -- credit risk, operational risk, reputational risk, strategic risk -- will be borne by the financial institution, not the vendor.

OCC Implementation of Initiatives

Implementation of the FFIEC guidance is the responsibility of the lead supervisors and, like our fellow regulators, we are taking aggressive action to implement the FFIEC initiatives. These are demonstrative of what our sister agencies also are doing.

Assessments. In conjunction with the release of interagency guidance in May, the OCC conducted assessments of every financial institution we supervise in order to gauge the institution's readiness for the task ahead. This general assessment helps us focus our resources

on the institutions that require priority attention. We also assessed the degree to which large national banks are considering the year 2000 exposure of their largest borrowers, and the banks' preparation for the new European Monetary Union currency, the Euro, which may compete for resources with year 2000 efforts.

Our finding was that some national banks and some vendors need to speed up their efforts in order to complete their year 2000 preparations in a timely manner. In order to alert institutions to the importance that both regulators and the Congress place on these preparations, and particularly the importance of setting and meeting deadlines, I recently sent a letter to all Chief Executive Officers of national banks and bank vendor companies expressing my concerns about those who are not doing enough.

To follow up on our assessments, OCC examiners contacted the Chief Executive Officers of each of the banks and vendors that we found to be lagging in their planning efforts. Examiners evaluated any actions taken since the first assessment. For banks that had not taken sufficient action, we scheduled an on-site examination within 90 days.

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 looked at syndicated loans exceeding $25 million in which the 24 largest national banks participate. Those banks underwrote approximately $425 billion in syndicated loans in 1996, representing 80 percent of the syndicated loans originated by national banks and 36 percent of all outstanding shared national credits.

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. Presently, most banks we have assessed are in the process of determining what should be done to address year 2000 credit risks. Most will review year 2000 plans with corporate borrowers, and many plan to include year 2000 analyses in their file documentation or credit review process.

European Monetary Union. The OCC has talked to a number 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 assessed said that their EMU projects conflict with their year 2000 projects. We will continue to monitor this issue.

Bank Examinations. The OCC is examining, on-site, every national bank for year 2000 compliance by mid-1998. 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 we would focus special attention on whether senior management and the board of directors are fully engaged in the planning and monitoring of year 2000 conversion efforts.

We initiated the examination process in June, and we have completed approximately 500 examinations. Based on our initial analysis of those exams, I can tell you that we are finding both evidence of strong commitment, and areas of concern. Overall, national banks are aware of the year 2000 problem, and, where relevant, are working well with their vendors. However, some banks, particularly some community banks, still do not have well-developed management processes for dealing with their vendors.

The banks that came up short in our initial examinations are on notice that they are behind schedule and will be held accountable to demonstrate improvements as soon as the next quarter. The OCC is instituting a quarterly reporting system for year 2000 monitoring of national banks and their vendors. This will enable more timely and efficient supervisory responses to institutions that are having year 2000 difficulties.

Enforcement. Institutions must recognize that making adequate preparations for the year 2000 is more than a regulatory requirement -- it is a business imperative. As part of our efforts to help make sure national banks are prepared for the date change, the OCC must consider how it will use its supervisory and enforcement authority if a bank fails to prepare adequately. Our response will, by necessity, depend on many factors. When we find that an institution is slipping behind schedule and is likely to fail to meet one or more of the key benchmark dates, we must identify the reason for that failure and assess the efficacy of enforcement action. We will not be hesitant to take action, but we must all recognize that doing so will not assure year 2000 compliance for institutions that are trying, but still failing, to solve their year 2000 problems. Thus, we are working with our fellow financial institution regulators to identify as early as possible which institutions are in serious trouble and to develop contingency plans to deal with them.

With regard to the service providers and vendors national banks use, we have successfully exercised enforcement authority in the past. In all such cases the service providers agreed to take corrective measures and it was not necessary to initiate formal proceedings. We have no reason to expect resistance from vendors with regard to our year 2000 efforts.

Outreach. I have asked senior OCC management to maintain an active role in communicating year 2000 issues and concerns to the industry. A discussion of the year 2000 is on the agenda for the “Meet the Comptroller” meetings with senior bank officers, which we hold throughout the year. Our district management teams have been very active in discussing this issue with their bankers during outreach meetings, and senior OCC managers will continue

to give speeches on this subject in a variety of public and industry forums. As the year 2000 approaches, we will also identify other useful ways to inform the public about these issues, while continuing to maintain public confidence in the banking system.

CAMELS Ratings. Your letter of invitation asks whether year 2000 preparedness will be reflected in an institution's CAMELS rating. Our examiners evaluate a bank's ability to manage risks, including the risks posed by existing or emerging issues facing the institution or the financial services industry, such as the year 2000 problem. In that regard, bank management's near-term year 2000 compliance efforts -- that is, how we rate their current year 2000 commitment -- will be a significant factor in determining the management component of the institution's safety and soundness CAMELS rating. Ultimately, an institution's failure to address the problem of, and prepare for, the year 2000 could lead to undue exposure to transaction, credit, liquidity, and strategic risks. Should it become clear, based on the results of testing, that an institution faces serious problems in making its mission critical systems year 2000 compliant, we would make appropriate adjustments to the capital and earnings components of the institution's CAMELS rating.

Contingency Planning Addressing Liquidity. As you note in your letter of invitation, problems can arise despite the best preparation. For that reason, we are also making sure, in the course of our examinations, that national banks have adequate contingency plans. Your invitation letter asks, specifically, what planning is necessary to handle the liquidity problems that may arise. The OCC as a matter of course evaluates liquidity risk and contingency funding plans during bank examinations. Based on their risk exposure and size, banks have either formal or informal contingency funding plans incorporated into their management processes.

However, the century date change could result in problems of a greater magnitude and of a somewhat different character than we have experienced in the past. If an institution was unable to access its data processing systems for an extended period of time, it would, eventually, be unable to conduct its business. Or, even if it could conduct its business, it might not be able to access its contingency funding lines, because its information systems could not communicate externally. Early testing, so that problems can be isolated and targeted contingency plans developed, is an essential element in dealing with this problem.

International Preparedness

Your letter of invitation asks about the year 2000 preparedness of the international community. The Federal Reserve Board, the Federal Deposit Insurance Corporation, and the OCC have been closely involved in efforts to focus the international supervisory community on the issue, recognizing this is a problem of global dimensions. In particular, both the Federal Reserve and I asked that this matter be put on the agenda for the Basle Committee on Banking

Supervision. I personally participated in that discussion. The Committee has just issued a paper on the year 2000 that outlines the steps that financial institutions need to take to resolve the problem, and identifies the role of bank supervisors in helping to ensure success. The Basle Committee has sent copies of this paper -- which covers much of the same ground as the FFIEC's statement -- to banking supervisors in more than 150 countries. A task force under the Committee is now surveying the adequacy of year 2000 efforts, both in G-10[7] and non-G-10 countries.

CONCLUSIONS

In my role as chairman of the FFIEC, I have worked with the other banking agencies to develop an aggressive program to address the year 2000 problem. We have informed the institutions we supervise about supervisory concerns and potential problems. In addition, the OCC and the other supervisory agencies have pressed for an international understanding of the need to provide similar uniformity and coordination among countries.

As Comptroller of the Currency, I have established a forceful program to ensure that national banks are prepared. A critical aspect of this program is testing. Banks must test their systems to make sure they can process dates after the year 2000, and they must make sure these systems are compatible with external systems with which they exchange data.

In conclusion, all the financial institution regulators are working hard to help the financial services industry succeed in meeting the year 2000 challenge. No banking supervisor can guarantee that no problems will occur on January 1, 2000. But we can -- and must -- do everything in our power to ensure that the institutions under our supervision understand what the situation demands, respond accordingly, and have contingency plans in place in case of malfunctions. As chairman of the FFIEC and the Comptroller of the Currency I am completely committed to that goal.

[7]The G-10, or Group of Ten, includes the following countries: Belgium, Canada, Germany, France, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom, the United States.