

Nine Obstacles to Overcome Y2K Problem in U.S. Banking Industry

Sangjin Yoo* Choongkwon Lee** Kumari Ryali***

요약 곧 다가올 서기 2000년이 되면 많은 프로그램들이 작성 될 때 고려하지 못했던 연도 인식문제로 인하여 정보시스템을 개발해서 운영하고 있는 많은 조직들이 고통을 겪을 것으로 예상되고 있다. 특히 금융계는 정보시스템이 업무에서 차지하는 비중이 비추어 볼 때 사소한 문제라도 엄청난 파장을 일으킬 것으로 믿어진다. 이러한 의미에서 본 논문은 미국의 금융계가 소위 Y2K라 불리는 서기 2000년 인식상의 문제를 극복하는데 우선 고려해야 할 9 가지 장애를 소개하고자 한다.

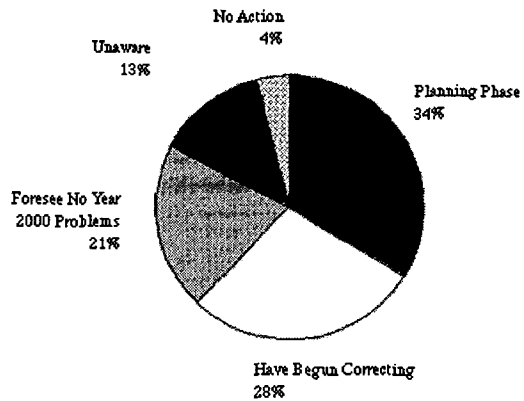
Abstract This paper discusses the threatening problem of Year 2000 (Y2K) to the banking industry. Of all steps to prepare for this big challenge, the clear understanding of the problem is always first to cope with the coming crisis. We categorize the possible issues into nine facets: (1) Potential Systemic Issues; (2) Technology Problems; (3) Technical Resources; (4) Vendor Management; (5) Supervisory Coordination and Security Issues; (6) Spillover Business Risks; (7) Operational Problems; (8) Euro Problem; and, (9) Face Closure or Loss of Federal Deposit Insurance. We believe that each of these nine issues must be clearly recognized and appropriately prepared by those bankers who want to avoid the disaster they have never experienced.

1. Introduction

The Y2K problem is a serious threat to the world economy. It is inevitable that it could disrupt the entire global economy in several ways. Specifically, the year 2000 poses a significant challenge for financial institutions because many automated applications will cease to function normally as a result of the way date fields have been handled historically. Unfortunately, most of human beings could not recognized until recently. The Figure 1 shows the status of Year 2000 awareness in the industry.

Now, we are facing the new millenium only with expectations without secured preparedness. But a number of authors suggest that we aware the coming challenge driven by Y2K problem, which is intrinsically initiated by ourselves.

<Figure 1> Status of Year 2000 Awareness



Source: Survey by Olsten Corp. (April 1996)

2. What Exactly is the Y2K problem?

In a nutshell, the Y2K problem is that many information technology systems in business today will

* Professor of MIS at Keimyung University

** Southeast Missouri State University

*** Southeast Missouri State University

not process information or won't process it correctly with dates beyond December 31, 1999. The problem stems from the way software developers decided to store dates in the early years of computers, when memory was many times more expensive than it is today. In those days, programmers stored the year as a two-digit number (e.g., 98) instead of a four-digit number (e.g., 1998). The problem is that when the next century arrives, computers may interpret the date "00" as "1900" and come to a halt. Just as bad or worse, they may continue to run but to produce incorrect results when comparing dates, performing arithmetic operations on dates, or sorting by date. The threat of breakdown requires us to modify millions of lines of code, to reentry a great deal of data in database, and to spend billions of dollars on scrutinizing all kinds of possibilities.

3. Banking Industry

Banking industry represents over 9,000 institutions with diverse business charters and geographic profiles. Banks are among the heaviest users of information technology. Because of this, they have been among the first to address the Y2K problem. Due to the close interdependency of the industry, banks must interact with regulators, service bureaus, other banks, Federal Home Loan Banks, secondary market agencies, commercial credit customers and foreign currencies and clients. Each of these links in the chain represents a potential Y2K disaster. Banking industry is not completely dependent only upon computer systems for processing transactions and storing data, but it also involves dates in that they are fundamental to banking (Wilson 1998).

Date-sensitive calculations such as those related to interest rates, due dates, pensions, benefits, and investments would be based on erroneous data. Inventory, maintenance and file retention could also be affected. In the worst case scenario, system failure crashes could result. Banks are at risk with any systems that calculate interest charges on various banking products, process credit or ATM cards, charge interest for late payments, or use dates for any calculations or comparisons (Harrison & Lonborg 1996).

Banks are now facing their greatest threat in history, namely, a dual domino effect: (1) bad data imported from other banks' computers; and (2) bank runs by frightened depositors (Anonymous 1997). The threat of the first will lead to the second.

4. What Happens When a System Runs into One of These Ambiguous Dates?

It depends on the application, the development language, the operating system, etc. Some examples of what might happen are (Morgan, J. P. Securities Inc. 1996):

- Your local bank may stop crediting your account with the proper interest or may retire your outstanding obligations prematurely. This problem may also affect a financial service firm's ability to clear and settle trades on a T+3 (three days after the trade) basis as well as to process ATM and direct deposit transactions.

- It could cause automated teller machines to deny access to cash, bank vaults to close or open improperly, or bank statements to report erroneous data.

- On January 3, 2000 (the first business day), an accounting department may be unable to enter journal entries in its general ledger because a posting date is required and "00" is an invalid year.

- A food manufacturer that produces a vacuum-packed product with a four-year shelf life calculates an expiration date of "00" for its latest product run and issues recall notices to its retailers because the date is less than the current date. Worse yet, this could happen to the "rework date" on automotive parts; with automated just-in-time inventory systems, improperly returned parts could shut down an auto production line for days.

- Phone calls started just before the end of 1999 that carry over to 2000 could be billed as 52 million minutes long (60 minutes * 24 hours * 365 days * 99 years).

5. Threat to the Banking Industry? How?

According to the Basle (1997) Committee, the Y2K presents a number of very difficult challenges for the financial service industry, which relies heavily on effective computer communications between banks, external data networks, data processing centers, and their customers. Banks rely heavily on automation to manage information. It has many automated linkages and interdependencies with correspondents and customers. All of these interdependencies must be addressed and tested to assure that problems are not present. If automated applications failed to work properly, it would lead banks not to conduct business. The Y2K is particularly challenging because it is not just internal to a bank. For larger banks that deal in multiple currencies and provide wide ranges of products in many countries around the world, the challenge is particularly great because many of these applications are interdependent. Similarly, banks rely on third party service providers or vendors for many applications. These applications not only need to be made compliant but they must also be thoroughly tested within each bank to ensure that they perform properly for the particular environment.

Many calculations will either indicate that transactions have been open for nearly 100 years or produce negative numbers. New files may not be recognized as the most recent data, causing current files to be erased or archived as old data. These and other logic issues have the potential for causing problems for debt collection, aging of information, calculating interest rates, etc., and could significantly disrupt normal business operations. Also, when dates are compared, customer billings may change from charges to refunds and vice versa. Complicating the problem for global banks is that they must also program their computer systems to deal with a brand new currency, the Euro. The scheduled introduction of the Euro is placing significant competing demands on scarce technical resources for institutions active in that market. Banks are warned against taking on any new projects like merging with or acquiring a noncompliant bank. On the other hand, noncompliant banks are

advised to consider finding a compliant buyer as "an approach to contingency planning." Weak links in the payment chains could "rapidly affect others if payments fail to move as expected."

Without considering dates, a bank computer cannot calculate the interest due on a loan. Bank loan officers must access the risk of earnings losses and business failures of their borrowers who fail to be Y2K compliant. The G10 Basel Committee on Banking Supervision warns bankers to closely examine the compliance of their loan customers. In other words, "don't lend to businesses that might fail in 2000". This is good advice with potentially very bad economic consequences: Borrowers will certainly fail before that date if they are cut off from bank financing by their loan officers.

It is estimated that it will take a minimum of three days to change, test and implement each program using traditional manual methods. A company or bank with more than 20,000 programs will therefore require 60,000 man-days or over 300 man-years to make sure its systems is ready for the millennium. Industry consultants estimate that bank's fixing costs could amount to \$1 for each line of computer code they have. BankBoston has some 50m lines of code spread over 273 different programs. Even if banks renovated or replaced 100 percent of their date-related computer code, they still would be vulnerable. Whether the banking industry has the ability to rise to this challenge and avoid serious problems as the date change occurs will be determined by the actions that individual banks and the banking community more generally take between now and the year 2000.

6. Issues of Y2K in the Banking Industry

Addressing the Year 2000 represents a major and complex issue to manage. As organizations have developed their detailed plans, a group of issues have surfaced that deserve particular attention. While several of these issues have already been discussed above, they are highlighted in more detail here for a better understanding of the threats facing the banking industry in regard to the Year 2000 problem.

6.1 Potential Systematic Issues

Banks are at the heart of world payments systems. A Y2K related systems failure could cause a bank to breach legal obligations arising from its fiduciary and contractual relationships with customers. Potential systemic issues need to be identified. This problem is not an issue that will present problems only to those who fail to rise to the challenge. For large banks and industry "utilities" that serve the entire banking community by offering services or products not readily available elsewhere, problems focused in a single location could rapidly affect others if payments fail to move as expected. Potential weak links in the payment chains need to be identified as early as possible with appropriate contingency plans developed and followed as necessary. Bank computer systems interact daily with the computer systems of customers, correspondents, vendors, other financial institutions, clearing houses, and corporate borrowers.

6.2 Technology Problems.

• Technical resources

As Year 2000 approaches and the urgency of fixing problems increases, some experts believe that the limited availability of technical support will be a major obstacle to making systems Year 2000 compliant. Skilled technical resources are already scarce and will become even more scarce as the deadline approaches. Already salaries for certain specialists are rising and key staff are being bid away by other companies. Bonuses and special retention packages are being used in many institutions to address the turnover issue. Knowledge of market conditions for skilled programmers and developing programs to retain key personnel may be necessary to ensure that adequate resources are available throughout the project's life. Outside consultants are facing similar demands resulting in higher costs. Here, however, the issue is not just cost but also the quality (skill and integrity) of the consultant and the level of confidence one can have that the consultant will continue to exist if problems are encountered. As a result of all of these factors, many organizations are finding it necessary to

increase budget estimates, sometimes several times and often significantly.

• Testing

On May 5th, the Federal Financial Institutions Examination Council ("FFIEC") issued a press release to focus the banks attention on the critical issues that financial institutions need to address quickly to resolve Year 2000 computer failures in order to avoid major service interruption. The release strongly encourages banks to complete an inventory of core computer functions and set priorities for Year 2000 goals by September 30, 1997. It also encourages them to largely complete program changes, and have testing well underway for mission critical systems by December 31, 1998 (Deering 1997).

The Century Date Change project was initiated in the Federal Reserve System in late 1995, according to Mr. Kelly². The Fed is setting up an isolated mainframe data processing center for "testing out payments system applications." Testing with banks is targeted to begin June 1998.

Bank hardware and software must be tested in all internal and external systems, foreign and domestic, with which they interact, or electronic fund transfers might fail or banks' systems might be contaminated with corrupt data. All applications and systems need to be thoroughly tested in ways that simulate actual business activity. Such testing should include not only internal systems but also products and services purchased from service bureaus or vendors. Relying on someone else to test or certify a system can pose significant risks. Because system interfaces often vary from institution to institution, what works in one place may not work in another.

Literally dozens of programs exist and were written years ago by companies that no longer exist. Still, the truly labor-intensive part of the task is not in updating the code. That might be 15% of the total work, the real grunt-work is in testing and re-testing the applications, and double-checking how they interact as each succeeding program is revised. Updates to software programs sometimes have unpredictable results, particularly on other programs with which they share data. That's why each revision needs to be tested.

Testing is much more time-consuming than repairing noncompliant code. Majority of software programs is part of a bigger corporate, industrial, national and even global network. They often depend on input information generated by other programs. They must all remain compatible as they are fixed. A problem in one system could trigger a Domino Effect, which poses a great risk to all who fail to test whether their local compliant system is compatible with their global network.

Testing will also be more difficult than usual. First, there will be competing demands for test environments. New applications like those related to the Euro or replacing fractions with decimals in trading activities will require testing in current environments. Yet given the importance of these applications and their interdependencies with other applications that must be tested for Year 2000 compliance, strategies will have to be developed for testing in both current and Year 2000 environments. Test data will need to be specially developed. Because testing is primarily a business line activity, business line resources will be under heavy pressure.

American National's Mecca says her bank has tested most of its peripheral applications. Still, she acknowledges, "No one can be 100% sure. We've done everything we can do and tested it, but no one is going to really know until Jan 1, 2000."

- **Target dates.**

Target dates for testing are critical both internally and externally. All the money in the world will not stop January 1 2000, from arriving at the rate of 3,600 seconds per hour. There is not enough time to fix and test all the systems, with billions of lines of software code around the world, that need to be fixed. Many businesses, governments, and organizations have become aware of the Year 2000 problem only recently and may simply run out of time. As meaningful testing often requires testing internally and with external parties, the coordination of test plans with correspondents and large, active customers become very important to the institution. Indeed, setting priorities and internal target dates will depend to some extent on when external testing becomes feasible. Especially for larger institutions, payment systems,

clearance and settlement systems, and similar utilities, communicating test plans for applications having external interfaces becomes crucial for the industry-wide planning process. Failure to address this issue in a timely manner could cause banking institutions to experience operational problems or even bankruptcy and could cause the disruption of financial markets. As a result, banking institutions must take the necessary steps to ensure that problems and disruptions are minimized.

McIsaac (1997) states that in spite of the looming problem, the banking industry reacts with a slow, lethargic unfocused effort. Bill Gates has portrayed banks as 'dinosaurs', unable to embrace leading technology innovations and capitalize on rapid new product and market penetration. Eugene Ludwig³ said his office recently surveyed banks to get a snapshot of their readiness for the year 2000. The survey found that 85 percent of large banks already have programs in place. However, he said, many community banks "need to step up their efforts." "About 15 percent of smaller banks," Mr. Ludwig said, "are not aware of the effect the Year 2000 will have on their businesses." Another 20 percent, although aware of the effect, are just starting to address the issue.

For institutions that may be somewhat lagging in their Year 2000 efforts to date, the need to communicate meaningful target dates for testing poses a dilemma. Not communicating readiness dates for external testing now or indicating a date that is too far out in the future sends immediate indications to the financial community that the institution may be lagging in Year 2000 efforts. On the other hand, communicating a target date that appears acceptable but which might not be met runs the risk of having credibility questioned even more severely if the target is missed. Setting optimistic targets that barely make compliance possible may be only disguising the real problem and issue for the organization.

- **Compliance**

To be fully compliant, all institutions will need to assess their computer software and hardware, change code that will cause processing errors, and test prior to implementation. All of these environmental and processing hardware and software projects will need to

be completed in order to conduct business as usual on January 3, 2000, the first business day.

The FFIEC has committed to on-site examinations of every bank, thrift and credit union for year 2000 compliance by mid-1998. It has emphasized that it would look for comprehensive planning and a clear commitment to meeting year 2000 goals. The G10 Basel Committee on Banking Supervision sent a wake-up call to the global banking industry on September 8, 1997 in a memorandum titled "The Year 2000: A Challenge for Financial Institutions and Bank Supervisors." It advises bankers to move decisively and immediately become compliant or face almost certain business death. The risks associated with non-compliance - credit risk, operational risk, reputational risk, strategic risk - will be borne by the bank, not the vendor. In the event that a vendor cannot meet established deadlines, contingency plans should be in place to change vendors, complete work internally, or otherwise adjust to vendor failure (Ludwig 1998).

The Fed is prepared to function as the data processing vendor of last resort for financial institutions that are 'unable to access their own systems.' The FED would join other banking agencies in the takeover of any banks that become insolvent as a result of Y2K. The Basel Committee observes that if a bank fails to fix the Y2K problem, it will face dire consequences.

• Certification

Certification has been a recurring and confusing issue for many institutions. Many institutions and especially smaller institutions believe that if a vendor certifies a particular product as being Year 2000 compliant, they need not worry about it. There are two fallacies to this idea. First, some vendors indicate that their product is compliant when in fact it is not. Second, even if the product is compliant, it still must be tested by the institution to make sure that it runs properly within the institution's own environment and interfaces properly with other applications.

6.3 Vendor Management

Banks that rely on outside vendors for critical

computing services have an extension until March 31, 1999, for completing the Year 2000 tests. Many smaller banks rely heavily on vendors for data-processing services and software. According to interagency guidance from the Federal Financial Institutions Examinations Council (FFIEC), banks that depend on vendors for critical operations such as posting deposits or sorting checks must carefully monitor their vendor's conversion efforts. Third party vendors pose special risks because the amount of oversight and control that an individual bank can influence is limited. Every bank must meet its timetable for compliance, whether data processing is performed in-house or by an external vendor.

According to a Circular No. 10937 (1997) by Federal Reserve Bank of New York, the agencies find that some financial institutions, relying on third-party data processing services or purchased applications software, have not taken a proactive approach in ensuring Year 2000 compliance by their vendors. Management should evaluate vendor plans and actively monitor project milestones. Institutions should determine if vendor contract terms can be revised to include Year 2000 covenants. It should also be aware of vendor specific responsibilities and their institution's vulnerability if the vendor cannot meet contractual obligations. In addition, it must also ensure that vendors have the capacity (both financial and personnel) to complete the project and are willing to certify Year 2000 compliance.

6.4 Supervisory Coordination and Security Issues

Policies regarding Year 2000 risks are being coordinated closely by Federal banking supervisors. Security issues arise and will become more pressing as the urgency of the Year 2000 increases. Normally sound security controls may be relaxed as consultants and subcontractors for consultants undergo less rigorous background checks before being granted access to bank systems and records. Date dependent security applications may be turned off to facilitate testing. As businesses focus more on resolving interconnectivity concerns, resources normally focused on security controls may be diverted.

Royal Bank of Canada's biggest challenge lies in

the desktop software it has deployed over the years to its corporate customers for applications like payroll, treasury workbench, and cash management. Virtually none of this software was Y2K compliant. It is now addressing Year 2000 dependencies for the 25,000 corporate clients with whom the bank exchanges data files (Darling 1997).

6.5 Spillover Business Risks

Spillover business risks and opportunities represent an area that is often overlooked when developing Year 2000 plans.

- **Data exchange**

The Year 2000 problem also poses a risk to the quality of information that institutions exchange with other firms. The international dimensions of the problem are a serious concern to bank regulators because of these interconnections. Large volumes of date sensitive data are transferred electronically between financial institutions, their customers, and their regulators. Institutions will need to know how methods of data exchange differ among financial institutions, across vendors, and between other institutions. Therefore, Year 2000 planning should allow sufficient time to assess the effect that Year 2000 solutions will have on data transfers. The project plan should also include testing and verification, as appropriate, of data exchanges with clearing associations, governmental entities, customers and international financial institutions (Interagency Statement 1997).

- **Special risks for certain institutions**

Remote or overseas operations also need to devote attention to Year 2000 issues. All banking units and locations should ensure that plans adequately cover systems and tools that are used to support operations, risk management, and control environments.

While inventorying mainframe and other applications under the control of a centralized information systems management may be relatively easy, departmental applications unknown to the centralized operation are increasingly common. Many of these applications are essential risk monitoring and business decision tools.

Extra effort is needed to identify these applications and make certain that they are compliant. To the extent that such systems serve as critical controls for business operations, they could expose the financial institution to significant undetected vulnerabilities. Appropriate staff members throughout the organization must be aware of the risks associated with the Year 2000 issue and how they might be affected (Interagency Statement 1997).

- **Corporate customers and increased liquidity risk**

Corporate customers (borrowers), who have not considered Year 2000 issues, may experience a disruption in business, resulting in potentially significant financial difficulties that could affect their creditworthiness. If loan customers or bond issuers cannot repay their debt as agreed, a bank could face increased transactional or credit risks. Some analysts fear that these problems could ripple throughout the world economy.

Banks should develop processes to periodically assess large corporate customer Year 2000 efforts and may consider writing Year 2000 compliance into their loan documentation. They should also consider in their credit analysis whether the borrower's Year 2000 conversion efforts are sufficient to avoid significant disruptions to operations. This is of significant importance as failure of customers to make the necessary adjustments can lead to a loss of business, loss of asset values for the bank, and pose credit and liquidity risks to the banks. Current financial performance will not be an indication of future performance for organizations that have not developed sound plans and provided for appropriate resources to carry them out (Interagency Statement 1997).

Comptroller of the Currency Gene Ludwig said that banks have to worry about whether their borrowers will be affected. He noted that there are estimates that business failures will increase by 10% as a result of such problems, and bankers must take steps now to minimize the risk that loans extended today will not turn sour on January 1, 2000. Ludwig admonished banks that their competitors will not hesitate to take advantage of and advertise the failure of banks to make timely interest payments or miscalculate dividend or maturity dates due to a Year 2000 error. Royal

chairman John Cleghorn has said his institution hasn't deemed it necessary to set aside any Y2K related reserves. He said each borrower's risk pattern will be closely monitored and a risk value placed on each one. If a particular client does not have a Y2K plan, their internal credit rating will come down (Marotte 1998).

Managing the risks in a commercial loan portfolio involves setting up a program to evaluate four aspects of each loan. First, if the borrower became delinquent or were to default how seriously would the bank be affected? Second, how seriously could Year 2000 problems affect the borrower? Third, how well is the borrower dealing with these risks. Finally, how can the bank best minimize its exposure to Year 2000 risks?

According to Golter and Hawry (1997), to assess each bank's credit-risk exposure to Year 2000 problems, it is necessary to understand the operational risks that Year 2000 creates for a bank's borrowers. These risks are like ripples in a pond, moving outward from the center of the firm's operations. The central risk lies in the firm's computer systems that handle core applications. These functions traditionally were housed on mainframe systems, but recent developments in data processing have moved much of this activity onto other platforms. The second circle of risk encompasses networks and PCs that may be important in the day-to-day operation of a firm. The third circle of risk involves exchanges of data with third parties. The fourth represents equipment built around microprocessors that operate with internal calendars. Extending outside the company, the fifth circle is composed of business partners, those organizations that provide essential services or are key customers of the firm. Finally, the sixth circle of risk is represented by the macroeconomy which may be adversely affected by the disruptions that result from efforts to adjust to the uncertainties posed by this unprecedented challenge and from the failures of some to prepare successfully for the date change.

The bright side of the Year 2000 issue is that it can also be a survival issue for customers. Having a strong Year 2000 program may open strategic opportunities to market the readiness posture of the institution.

In any event, credit and relationship officers should

already be cognizant of their customer's readiness, tracking progress over time, estimating possible business ramifications if customers fail to become compliant, and developing contingency plans as appropriate (Interagency Statement 1997).

• Mergers and acquisitions (M&As)

Mergers and acquisitions represent another area where Year 2000 readiness should be taken into account. Such activity would place additional burden on scarce technical and managerial resources of the organizations. The rush of bank mergers and acquisitions has increased the vendor conversion workload. The extent of Year 2000 conversion efforts will bear directly on corporate M&As' strategies since conversions resulting from M&As will compete for project managers and technical resources (Circular No.10937 1997).

For organizations that are stretched in meeting Year 2000 compliance, acquiring another institution would be highly risky. Banks, whose every product line, customer service and internal accounting program must be adjusted, would rather sell than spend on the necessary upgrades. At some point the banks may not be willing to bear the cost or have the time to do it but the merger game is going to go on irrespective of the year 2000. Banks may become willing sellers, but buyers may not be willing to make a move past a certain date. However, the possibility of being acquired might be an approach to contingency planning.

At minimum, rigorous diligence on Year 2000 preparedness should be conducted in order to assess the status of the institution being absorbed and how the combined institutions would affect Year 2000 plans, actions and ultimately readiness. As time passes, there is decreasing ability for any organization to absorb a non-compliant one and make the necessary changes before the century date change. Therefore, banks that want to do acquiring must move now.

6.6 Operational Problems

Failure to have operational automated systems can prevent even simple business functions from being completed because manual or other alternatives may not be feasible if processing volumes are sizable or

information exchanges are extensive.

• **Legal and liability**

Legal issues may arise from the lack of specificity in contract terms dealing with Year 2000 issues. Financial institutions should modify existing contracts that do not specifically address Year 2000 compliance by the vendor. Current and future purchases should require Year 2000 certification. If contract changes or modifications are refused, then the institution should consider replacing the service or product. Otherwise, conflicts may result regarding the commitment and responsibility to assure Year 2000 compliance (Interagency Statement 1997). Consultants estimate that legal costs alone could be in the hundreds of billions of dollars if problems are extensive in the industry. Such estimates clearly suggest the magnitude of the strategic risk faced by a bank and the industry more generally.

If undetected or uncorrected, Year 2000 problems could cause a bank's systems to fail. The bank, along with its directors and officers, could unknowingly breach many legal obligations arising from its fiduciary and contractual relationships with customers.

• **Replacement vs. Repair**

Cost and timing are two factors that will affect a financial institution's decision to replace or repair strategic systems. Those factors may dictate that some systems will be repaired in the short term and strategically replaced sometime after January 1, 2000. Conversely, it may be more cost effective to accelerate the replacement of strategic systems (Interagency Statement, 1997).

• **Leap year**

All Year 2000 plans need to address the leap year - February 29, 2000 - issue. All date and calculation routines need to be reviewed to ensure that leap year calculations are Year 2000 certified (Interagency Statement 1997).

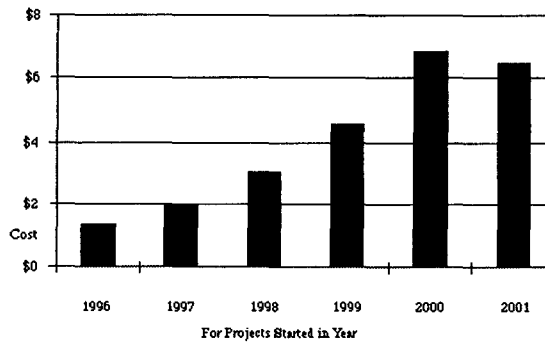
• **Cost control and monitoring**

The Year 2000 problem is an expensive one because of four primary reasons: the persuasiveness of the problem, the multiple solutions that potentially solve

the problem, the significant role testing plays in solving the problem, and the legal and liability concerns associated with the Year 2000. The costs that the banking industry will need to incur to address the Year 2000 are extensive. Westergaard anticipates Year 2000 costs to arise from the following four sources: internal staff costs, consulting, other expenses, testing and conversion of system applications (Westergaard 1997). Many organizations appear to be underestimating the costs of testing by not recognizing that many tests will have to be performed multiple times as vendors change releases or operating systems environments or applications change. Additionally, business line management often fails to recognize that the largest share of the testing burden will ultimately fall to them.

Worldwide estimates of the Year 2000 problem are staggering. The Gartner Group quotes a global price tag of \$300-600 billion based on a cost of slightly more than \$1 per line of code, and "cost per line of code" is expected to grow by as much as 50% per year as the deadline approaches. Verification of this number is difficult since very little real-world experience with fixing the problem is available yet (Morgan, J. P. Securities Inc. 1996).

<Figure 2> Estimated Cost of Year 2000 Fixes (in millions)



Source: Consultants hired by J.P. Morgan.

- Estimated costs for every line of code in every program that needs to be reviewed are about US\$1 per line.

- Nations Bank Corp. said it will spend \$120 million over three years to fix its computer systems so they

can understand dates in the next millennium.

- The Charlotte, N.C. based bank said it spent \$25 million last year on Year 2000 issues.
- Citi Bank will spend \$600 million on Year 2000 over the three-year period from 1997 through 1999, of which approximately \$150 million was incurred in 1997 (Market Partners 1998).

Another significant reason for Year 2000 cost estimates being so high is concern over the lawsuits that will follow. USA today reported that "Litigation resulting from Year 2000 meltdown will be more costly than asbestos, breast implant and Superfund cleanup lawsuits combined." Total litigation costs could exceed \$1 Trillion.

• Community Banks Budget

To gauge the progress of community banks, Grant Thornton⁵, surveyed more than 5000 community bank chief executives. Some 600 banks, averaging \$155 million of assets, responded. Nearly 75 percent of the 600 community bank executives surveyed said they would spend less than \$10,000 this year upgrading information systems. According to a widely held view, banks need to spend \$100,000 per \$100 million of assets to make sure their computer systems do not crash and disrupt business on New Year's Day 2000. Of those banks, half said they planned to spend less than \$10,000 this year, compared with the 72 percent that spent at least as much in 1997. One-third said they anticipated spending less than \$5,000, only 8 percent have budgeted more than \$50,000 this year, one-fifth said they did not know how much they would spend and 5 percent said they would spend nothing. Insufficient budgets tell only half the story in the looming year-2000 crisis. The survey showed 44 percent of all community banks have yet to test their vaults and security systems for year 2000 problems. Only 37 percent have contingency plans if the systems fail and interrupt operations. Just 20 percent know how their major borrowers are addressing the year-2000 problem.

6.7 Outside Auditors and Public Reports

"Auditors at many banks and software companies

gather inventories of every last piece of software a bank uses," says Dan Murphy⁶. Outside auditors and public reports are likely to become an issue at the end of the current fiscal year for some organizations. In some countries like the United States, the decision has already been made that Year 2000 renovation costs must be accounted for in the year in which they are incurred. While the accounting profession is still debating whether such costs will have to be disclosed as a specific item, there is building consensus that organizations appearing to be unable to be Year 2000 compliant for material businesses or applications will have to have this risk specifically noted in certified statements. At what point such disclosure begins to be required remains uncertain.

6.8 Euro Problem

Banks now must brace themselves for another daunting - and very expensive - software-related problem, this one involving the new European currency known as the Euro¹. According to John Marks (1997), no later than December 31, 1998, bank transactions with Europe will have to rewrite their computer software to handle three different base currencies at once. The value of the Euro will have to be determined on a daily basis by its relationship to both the dollar and other European currencies. In other words, every bill, every financial statement, and every stock price in the ten or more countries set to join what is known as the European Monetary Union will have to be "triangulated."

The Year 2000 problem is compounded by the introduction of the Euro in January 1999, at a time when remedial measures to fix the problem will be at their height. Banks now face with Euro compliance. Euro compliance is more complicated and has more uncertainties than Year 2000 readiness. The Euro-driven choice for most banks is between forced consolidation or strategic alliances. The banks need to ensure that their existing products are "Euro-compliant" - that systems are ready to deal with the new currency. Institutions are under even greater systems and financial pressures because non-negotiable EMU and year 2000 preparations need to continue in parallel. It has been stated that 40

percent of banks have a high degree of readiness in the technical sense although none are totally prepared.

The two problems of Year 2000 and the Euro would seem to be unrelated. But the coincidence in timing - the millennium bug and the currency change arrive within a year of each other - has transformed them into a larger, single crisis for many banks. The twin costs of EMU and year 2000 compliance will increase pressure from shareholders to improve revenue from other sources in terms of added products.

6.9 Face Closure or Loss of Federal Deposit Insurance

According to an article by Matt Hamblen (1998), by early September 1998, some of the nation's private banks will face closure or loss of federal deposit insurance, if federal auditors find they can't fix year problems on time. The FDIC has already issued a "cease and desist order" against any institution whose board has done nothing, so far, to investigate whether its systems are Y2K compliant. Ironically, the agency that oversees those banks, the Federal Deposit Insurance Corporation (FDIC) has itself fallen eight months behind in its year 2000 preparations. Federal Reserve notified the chief executive officers of all U.S. bank holding companies that their institutions would be subject to "appropriate" enforcement actions if they were found to have Year 2000 liabilities and failed to take corrective actions. A closure would force banks to secure deposits and made sure they are returned to customers, much the same way federal authorities close a bank for insolvency or other problems. A Reuters story (1997), says that the FED may suspend all transactions with noncompliant foreign banks in 2000. This is tantamount to shutting down the international banking system.

7. CONCLUSION

The Year 2000 issue is potentially the biggest challenge ever faced by the financial industry. The Y2K virus has infected all the vital organs of our global body of the new year. The demand to establish bank focused Year 2000 consortiums and workgroups

must begin now. Emerging competitive campaigns by brokers and other financial institutions will target customers to question the safety of their investments in banks. This will deliver comfort to Congress, shareholders and customers that the U.S. banking industry is ready and has taken all reasonable measures to reduce the risks associated with the Year 2000 event. According to Gartner Group, U.S. banks are considered ahead of banks in nearly all other countries, which means international money transfers will be at risk. The Information Technology Association of America announced on September 22, 1997, that BankBoston⁸ has become the first financial institution to earn IT AA - 2000 certification. The certification indicates that the bank has the core capabilities needed to address the Year 2000 challenge.

Time is getting short for banks in the market for a new core system, and available conversion dates are filling up quickly. Achieving Year 2000 readiness in the banking industry is critical to ensuring the safety and soundness of the banking system. For this reason, promoting Year 2000 compliance by banking organizations is one of the highest priorities of the Federal Reserve's supervision program. The Fed's central bankers fear regional economic issues may distract European and Asian banks from dealing with the "millennium time bomb" threatening the world banking system. A banking organization's ability to provide uninterrupted services to its customers and to continue to comply with all applicable consumer protection statutes and regulations should be critical elements of a banking organization's Year 2000 readiness program.

Footnotes

[1] The Basle Committee on Banking Supervision is a Committee of banking supervisory authorities, which was established by the central bank Governors of the Group of Ten countries in 1975. It consists of senior representatives of banking supervisory authors and central banks from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, Netherlands, Sweden, Switzerland, United Kingdom, and the United States. It usually meets at the Bank for International Settlements in Basle, where its permanent Secretariat

is located.

[2] US Senate's Committee on Banking, Housing, and Urban Affairs, Federal Reserve Board Governor Edward W. Kelly Jr.

[3] Eugene Ludwig is the Comptroller of the Currency, chairman of the exam council.

[4] Royal Bank of Canada is the largest bank in Canada and the sixth largest in North America

[5] Grant Thornton is the national director of financial services for Chicago base.

[6] Dan Murphy is a senior vice president at Fiserv and the company's chief auditor.

[7] Euro is the new currency bloc in the European Economic and Monetary Union. The Euro will be introduced in January 1999. It will not become the sole currency in Europe until July 1, 2002. On that date, all other currencies will be taken out of circulation.

[8] Bank Boston, the 15th largest bank holding company in the United States, with assets of \$66.1 billion as of 6/30/97, began tackling the Year 2000 problem in early 1995 and expects to spend \$50 million on the solution. The project involves reviewing more than 60 million lines of code in 190 software applications utilized in BankBoston's worldwide operations. Forty people currently work full time on Year 2000 issues at BankBoston.

References

[1] Anonymous. (1997). The Domino Effect in International Banking. Gary's North's Y2K Links and Forums. Available at <http://online.guardian.co.uk/computing/880567375-bomb.html>

[2] Basle. (1997). The Year 2000, A Challenge for Financial Institutions and Bank Supervisors. Basle Committee on Banking Supervision. Available at <http://www.bis.org/publ/bcbs31.htm>

[3] Circular No.10937. (Apr. 4, 1997). Year 2000 Alert. Federal Reserve Bank of New York.

[4] Darling C. (1997). Royal Bank of Canada Investigates its Y2K dependencies. Datamation, Vol.

43. Issue 1. p. 44.

[5] Deering, A. (Apr. 6, 1997). Risk Management and the Year 2000. Managing Partner ADVICE, Inc. Available at <http://www.adviceinc.com/2000/2000-WP.html>.

[6] Golter, J. & Hawry, P. What Every Loan Officer Needs to Know about the Year 2000 Computer Problem (But Doesn't Know How to Ask).

[7] Hamblen, M. (1998), "Y2K Shortcoming May Shutter Some Banks. Computer World. Vol. 32. Issue 7. pp. 1-96.

[8] Harrison, J. S. & Lonborg, K. (1996). Get Ready for the Millennium. Texas Banking. Vol. 85. Issue 4. pp. 40 - .

[9] Interagency Statement. (May 5, 1997). Year 2000 Project Management Awareness. Federal Financial Institutions Examination Council.

[10] Ludwig, E. (Mar. 16, 1998). Year 2000 Watch. Year 2000 News. Available at <http://www.bankinfo.com/year2000.html>

[11] Market Partners. (Feb. 26, 1998). Citibank Will Spend \$600 Million on Year 2000. Available at <http://www.marketpartners.com/citibank.htm>.

[12] Marks, J. (Nov. 17, 1997). Latest Software Nightware, the Currency Change in Europe Could Cost U.S. Firms Billions. Business & Technology, U.S. News Online.

[13] Marotte, B. (Mar. 13, 1998). Banks Watch Borrowers as Y2K Nears. Business Ottawa Citizen Online.

[14] Morgan, J.P. Securities Inc. (Jul. 22, 1996). The Year 2000 Problem: Ready or Not, Here It Comes. Equity Research.

[15] Mclsaac, J. V. (Jul. 28, 1997). Millennium Success. Market Partners Inc., Version 2.2.

[16] Reuters Story. (Nov. 19, 1997). FED may bar transactions with Foreign Banks in 2000. Available at.

[17] Westergaard. (Jul. 29, 1997). Chase Manhattan Banking Corporation Reports Year 2000 Liability in its Annual Report Citing Hundreds of Millions of Dollars in Future Costs in its Annual Report.

[18] Wilson, C. (1998). May All Year 2000 Issues Not Be Forgotten. *America's Community Banker*, Vol. 7. Issue 1. pp.10-14.