

1999 SENATE INDUSTRY, BUSINESS AND LABOR

SB 2303

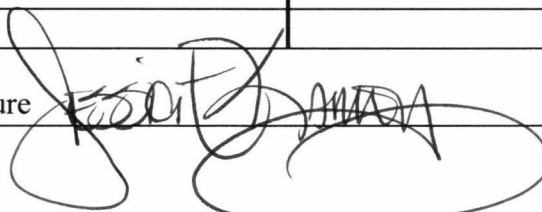
1999 SENATE STANDING COMMITTEE MINUTES

BILL/RESOLUTION NO. SB2303

Senate Industry, Business and Labor Committee

Conference Committee

Hearing Date February 2, 1999

Tape Number	Side A	Side B	Meter #
2	x		0-3528
Committee Clerk Signature 			

Minutes:

Senator Mutch opened the hearing on SB2303. All senators were present.

Jim Schlosser testified in support of SB2303. His testimony is included.

Marilynn Foss testified in support of SB2303. Her testimony is included. Senator Krebsbach asked her if they would have any problem with putting a sunset on the bill. She said that they would not have a problem with that.

Gregg Scheider testified in support of SB2303.

Shawn Cleveland testified in support of SB2303. Her testimony is included.

Jim Goetz testified in support of SB2303. His testimony is included

Joel Gilbertson testified in support of SB2303. His testimony is included.

Senator Mutch closed the hearing on SB2303.

Page 2

Senate Industry, Business and Labor Committee

Bill/Resolution Number Sb2303

Hearing Date February 2, 1999

Senator Krebsbach motioned to amend the bill. Senator Klein seconded her motion. The motion carried with a 7-0-0 vote.

Senator Krebsbach motioned for a do pass with amendments committee recommendation.

Senator Klein seconded her motion. The motion carried with a 7-0-0 vote.

Senator Mathern will carry the bill.

PROPOSED AMENDMENTS TO SB 2303

Page 2, line 19, replace the period with a comma and replace "Unless" with "unless"

Date: 2/2/99
Roll Call Vote #: 2303 1

1999 SENATE STANDING COMMITTEE ROLL CALL VOTES
BILL/RESOLUTION NO.

Senate INDUSTRY, BUSINESS AND LABOR COMMITTEE Committee

Subcommittee on _____
or
 Conference Committee

Legislative Council Amendment Number _____

Action Taken TO AMEND SUNSET CLAUSE, AMENDMENT

Motion Made By KREBSBACH Seconded By KLEN

Senators	Yes	No	Senators	Yes	No
Senator Mutch	X				
Senator Sand	X				
Senator Klein	X				
Senator Krebsbach	X				
Senator Heitkamp	X				
Senator Mathern	X				
Senator Thompson	X				

Total (Yes) 7 No 0

Absent 0

Floor Assignment _____

If the vote is on an amendment, briefly indicate intent:

Date: 2/2/99 SR21786
 Roll Call Vote #: 2303 2

**1999 SENATE STANDING COMMITTEE ROLL CALL VOTES
 BILL/RESOLUTION NO.**

Senate INDUSTRY, BUSINESS AND LABOR COMMITTEE Committee

Subcommittee on _____
 or
 Conference Committee

Legislative Council Amendment Number _____

Action Taken DO PASS AS AMENDED

Motion Made By KREBSBACH Seconded By KLEN

Senators	Yes	No	Senators	Yes	No
Senator Mutch	X				
Senator Sand	X				
Senator Klein	X				
Senator Krebsbach	X				
Senator Heitkamp	X				
Senator Mathern	X				
Senator Thompson	X				

Total (Yes) 7 No 0

Absent 0

Floor Assignment MATHERN.

If the vote is on an amendment, briefly indicate intent:

REPORT OF STANDING COMMITTEE

SB 2303: Industry, Business and Labor Committee (Sen. Mutch, Chairman) recommends **AMENDMENTS AS FOLLOWS** and when so amended, recommends **DO PASS** (7 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING). SB 2303 was placed on the Sixth order on the calendar.

Page 1, line 3, after "disruption" insert "; and to provide an expiration date"

Page 2, line 19, replace ". Unless" with ", unless"

Page 3, after line 5, insert:

"SECTION 8. EXPIRATION DATE. This Act is effective through July 31, 2003, and after that date is ineffective."

Renumber accordingly

1999 HOUSE INDUSTRY, BUSINESS AND LABOR

SB 2303

1999 HOUSE STANDING COMMITTEE MINUTES

BILL/RESOLUTION NO. SB 2303

House Industry, Business and Labor Committee

Conference Committee

Hearing Date 3-02-99

Tape Number	Side A	Side B	Meter #
1	x		0 - 59
1		x	0 - 8.3
3		x	18.4 - 25.6
Committee Clerk Signature <i>Lisa Horner</i>			

Minutes:

SB 2303 Relating to the financial institutions and credit unions for malfunctions or failures of computer or other electronic systems as the result of a year 2000 disruption and to provide and expiration date.

Chairman Berg opened the hearing on the bill.

Sen. Jerry Klein introduced and testified in support of the bill. He explained the Y2K situation relates much to financial institutions.

Sen. Deb Mattern testified in support of the bill. Computers have been replaced because of possible Y2K problem.

Jim Schloser testified in support of the bill.

(see attached written testimony)

Marilyn Foss, Gen. Council ND Bankers Association, testified in support of the bill.

(see attached written testimony)

Ekstrom asked what the federal government intended to do.

Foss said they would sue the bank.

The committee discussed the possible problems and ramifications that could surface because of Y2K problem.

Greg Tschider, ND Credit Union League, testified in support of the bill. He responded to earlier questions from committee members on the Y2K problems. Law suits relating to the Y2K will include actual out of pocket expenses. People will check their own accounts and will usually detect a problem in their bank accounts. Losses that are paid through law suits will only cover costs relating to actual problem costs. Pain and suffering will not be covered and agreed to.

Under ND law after 6 years if the money is not claimed it is lost to the state.

3 other states have passed this type of legislation.

Shawan Cleveland, BNC National Bank, testified in support of the bill.

(see attached written testimony)

Committee members asked her to explain some of the technical methods of addressing the Y2K problem. Cleveland said testing was done and Julian dates were used to tract possible problems.

All banks are required to do testing by the examiners.

Koppang asked about small banks.

Cleveland said they could stop you from doing business and even possibly sell a bank that does not take precautions.

Glassheim asked what could possibly happen if the bank failed due to Y2K problem.

Cleveland said interest calculations would be incorrect and systems could actually shut down.

Jim Goetz, Security First Bank of Oliver County, Center, ND, testified in support to the bill.

(see attached written testimony)

Joel Gilbertson, ICBND, testified in support of the bill.

(see attached written testimony)

Gary Preszler, State Banking Commissioner, testified in support of the bill. He responded to question by committee members about the problem of the Y2K problems. He said 1/3 of examinations in phase 1 were completed. The potential Y2K problem has affected the examinations.

Chairman Berg closed the hearing on the bill.

Tape 3, side B. Meter No. 18.4

Chairman Berg opened the discussion of SB 2303.

The banks are trying to take care of the Y2K problems that they could have with this bill.

Rep. Keiser made a motion for a Do Pass.

Rep. Severson second the motion.

The roll call vote was 14 yea, 1 nay.

The motion carried.

Rep. Severson will carry the bill.

Date: 3-2-99
 Roll Call Vote #: 1

1999 HOUSE STANDING COMMITTEE ROLL CALL VOTES
BILL/RESOLUTION NO. SB 2303

House Industry, Business and Labor Committee

Subcommittee on _____
 or
 Conference Committee

Legislative Council Amendment Number _____

Action Taken do pass

Motion Made By Keiser Seconded By Severson

Representatives	Yes	No	Representatives	Yes	No
Chairman Berg	/		Rep. Thorpe	/	
Vice Chairman Kempenich	/				
Rep. Brekke	/				
Rep. Ekstrom	/				
Rep. Froseth	/				
Rep. Glassheim	/	/			
Rep. Johnson	/				
Rep. Keiser	/				
Rep. Klein	/				
Rep. Koppang	/				
Rep. Lemieux	/				
Rep. Martinson	/				
Rep. Severson	/				
Rep. Stefonowicz		/			

Total (Yes) 14 No 1

Absent _____

Floor Assignment Severson

If the vote is on an amendment, briefly indicate intent:

REPORT OF STANDING COMMITTEE (410)
March 2, 1999 4:26 p.m.

Module No: HR-37-3892
Carrier: Severson
Insert LC: . Title: .

REPORT OF STANDING COMMITTEE

SB 2303: Industry, Business and Labor Committee (Rep. Berg, Chairman) recommends DO PASS (14 YEAS, 1 NAY, 0 ABSENT AND NOT VOTING). SB 2303 was placed on the Fourteenth order on the calendar.

1999 TESTIMONY

SB 2303

TESTIMONY OF MARILYN FOSS
On Behalf of the North Dakota Bankers Association
SB 2303

Mr. Chairman, committee members, I am Marilyn Foss, general counsel for the North Dakota Bankers Association. I am appearing before you today to support SB 2303 and to explain its specific provisions, as you've already had an overview of the problem and how federally insured financial institutions have prepared and continue to prepare to meet the millennium.

Let me begin by telling you that this bill is not an "immunity" bill. It isn't intended to shield dilatory banks, thrifts or credit unions from liability for monetary losses which a customer may experience if there is a Year 2000 disruption with an institution's computer systems. It also doesn't shift liability which is properly that of the financial institution or credit union to other parties. However, it is intended to establish a reasonable framework for Year 2000 lawsuits where an insured financial institution or credit union is the defendant and to focus the issues and narrow the liability of institutions which qualify for the bill's limited protection.

Definitions - Section 1 simply defines a few terms which are used in the balance of the bill.

How does a bank, thrift or credit union qualify ?

This is set out in section 2 of the bill. First, the defendant financial institution or credit union must be covered by federal deposit or share insurance which protects customer's deposits/ shares up to the amounts provided by federal law. Secondly, the institution must have a Year 2000 readiness plan and must have made a good faith effort to have implemented the plan. Insured institutions have been operating under a federal regulatory mandate to develop and implement Year 2000 readiness plans. By now, banks and thrifts and, I understand, credit unions, have been examined at least once for their compliance with the federally imposed standards

for readiness. (The standards have required institutions to evaluate their equipment and software, to establish deadlines for correcting problems which are discovered, and to set deadlines for the completion of multiple tests of their systems. In 1999 the focus of the federal requirements is testing, contingency plans, and customer preparedness.) This year our banks and thrifts can expect multiple, regulatory examinations of their Year 2000 readiness. Institutions which do not meet the requisite level of preparedness can be subjected to the full panoply of enforcement options ranging from the imposition of cease and desist orders with the attendant financial penalties for non-compliance to actual closure. These sanctions are not idle threats; there are institutions in other states which have already been subjected to well publicized cease and desist orders and there is no reason whatsoever to doubt the existence of a hammer behind the regulators' promises of vigilance about Year 2000 readiness. Under the bill, institutions which are substantially in compliance with regulatory requirements are conclusively presumed to have met the standard for good faith. (In this vein, the standard of good faith is tougher than that which we understand has been proposed as adequate to give the state Immunity - because of the condition for substantial compliance with the federal mandates.)

When must an action be brought? We are proposing to have a one year statute of limitation when an insured financial institution or credit union is sued as a result of a Year 2000 disruption. Our thought is that the fact of a disruption will be known very early in 2000 and that any lawsuits should be started without much delay. Accordingly, section 3 of the bill requires these lawsuits to be commenced by January 1, 2001.

Who are the potential parties? Section 4 of the bill limits these lawsuits to persons who are in "privity of contract" with the defendant financial institution or credit union. "Privity of contract" is a term of legal art. Persons who are in privity of contract have an agreement with one another for products or services. The privity

of contract requirement limits the class of persons who are potential plaintiffs in these lawsuits to customers of the insured financial institution or credit union. Customers of a customer are not permitted to sue.

How are damages addressed? The point of the bill is to limit liability for damages but to allow actual, monetary damage awards against insured financial institutions or credit unions. If a customer loses money because of a Year 2000 disruption which is caused by an insured financial institution or credit union, the customer is entitled to recover damages. So, what are the limitations in the bill? They are derived from tort reform which was enacted in 1995:

Actual Economic Damages - Damages which may be recovered are limited to actual, economic damages under sections 5 and 7 of the bill. Actual, economic damages means monetary losses. The term excludes consequential damages, extraordinary damages, non-economic damages (e.g., loss of enjoyment of life, emotional distress, pain and suffering) and damages for projected losses of future income or earnings and lost future business or employment opportunities. Punitive damages are also excluded.

Comparative Responsibility - One of the issues which has come increasingly to the forefront is that of customer and other third party preparedness. Section 6 of the bill addresses this issue in two ways. First, in a concept taken directly from North Dakota's tort reform laws, it is provided that a plaintiff's contributory act or omission doesn't bar recovery unless the act or omission was as great as the combined responsibility of every other person whose conduct contributed to the economic damages. But the damage award is to be diminished in proportion to the contributing conduct of the plaintiff. A jury may be required to allocate responsibility among the parties.

Additionally, where several persons contribute to Year 2000 disruption damages and are liable for them, the liability of an individual is several only. This means that

no defendant ends up paying damages beyond the proportion of contribution allocated to that defendant by the court or jury. **This is an elimination of joint and several liability and is also a concept which is taken directly from North Dakota's tort reform laws (Ch. 32-03.2, N.D.C.C.)**

It is our view that the limitations of liability which are embodied in this bill are appropriate for insured financial institutions and credit unions which have made a good faith effort to be ready for the Year 2000. The bill does not immunize anyone from a lawsuit or liability and it does not foreclose any customer from recovering monetary losses which occur as a result of a Year 2000 disruption. What the bill does require is for Y2K lawsuits to be brought promptly and to be highly focused - on what money was actually lost and, whose conduct contributed to a loss. Ultimately, insured financial institutions and credit unions are held responsible for the monetary losses to which their conduct contributed or caused.

Thank you.

SB 2303
Senate Industry, Business & Labor Committee
Comments by Jim Schlosser, Executive Vice President
North Dakota Bankers Association

Year 2000 Glitches

We can trace the Y2K problem back to "tabulating equipment" that businesses and government agencies relied on before computers became common in the 1960's and 70's. The tabulating machines read, sorted and tallied information entered on millions of envelope-size cards. Each card held only a small amount of information so abbreviations and codes were used for words and numbers. For example, typists recorded the year 1955 onto a card by punching holes for "55". The same shorthand method continued in the computer age because of costs and storage problems with early computers before the invention of computer chips. The two-digit arrangement for calendar years worked fine until now. On Jan. 1, 2000, if the date is simply recorded in a computer as 00, the computer assumes it means 1900, not 2000, unless the computers and computer chips are reprogrammed.

What financial institutions have been doing to prepare for Year 2000.

North Dakota banks, thrifts and credit unions, whether large or small, have been preparing and testing for the year 2000 for approximately three years. **Financial institutions are the only businesses that have year 2000 state and federal regulatory requirements** (see attached article). Federally-insured financial institutions in the state have tested their systems, written contingency plans, have been and will continue to be examined through 1999 (quarterly Y2K examinations are scheduled). It is estimated that \$8 billion has been spent to date by financial institutions in the United States to prepare for Y2K and banks are rated number one in Y2K preparedness by leading computer industry experts.

North Dakota's Attorney General called a press conference on Jan. 21 to urge North Dakota residents to "keep their money in the bank". A theme has been adopted in a joint effort with the North Dakota Bankers Association "There is nothing safer than money in the bank" (see attached flyer). The Attorney General is quoted as saying "your money is safest in the bank" and the Commissioner of Banking recently stated before a House appropriations subcommittee, "North Dakota financial institutions should be fully prepared for the century date change and I expect very little disruption, if any, to customers."

North Dakota financial institutions are required by federal regulators to have a special contingency plan in preparation for the year 2000. Banks and thrifts have contingency plans at the present time, which worked very well during the extensive flooding in the Red River Valley in 1997. Banks and thrifts that lost buildings due to the flooding and fire on Saturday were handling transactions and processing checks on the Monday following the disaster.

Legislation dealing with state and political subdivisions.

The interim Information Technology Committee and the Legislative Council introduced House Bill 1037, which gives the state and political subdivisions immunity for any claims arising out of the failure of computer hardware or software if the state or political subdivision has made a "good-faith effort" to make the hardware, software and computers comply with the year 2000 date change.

While attending this hearing, I was encouraged by the position of the trial lawyers on this issue. While a representative of the Trial Lawyers Association stated there should not be complete immunity by the state and its political subdivisions, he did agree that legislation is necessary to limit damages resulting from outside businesses and agencies causing damages because they are not Y2K compliant. The Trial Lawyers argued that if a state or political subdivision had met the test for compliance, evidence could be offered by the claimant to rebut this presumption. SB 2303 does fit within the guidelines established by the trial lawyers in their testimony before the House Government and Veterans Affairs Committee on HB 1037.

Why is this bill necessary?

Financial institutions in this state have invested an unprecedented amount of resources to achieve year 2000 readiness, and are doing so under the strictest scrutiny of federal and state regulators, congressional oversight, financial markets, the press and millions of customers. The goal of the enormous effort is a smooth transition into the next century for all banking services.

As financial institutions proceed to finalize the Y2K preparation, it is increasingly clear that they may face another expenditure that is even larger than the \$8 billion being spent by the industry on Y2K readiness — and that would be the cost of litigation brought by individuals or class action plaintiffs seeking damages for alleged Y2K disruptions. While financial institutions are confident that they would be successful in defending these actions, the costs of defending frivolous lawsuits would be passed on to their customers.

Financial institutions are not seeking some limitation of liability because they are not prepared. In fact, most financial institutions are well ahead of the government-mandated deadline of testing of all systems by June 30, 1999. There is inter-dependency between the systems used by financial institutions and external interfaces. We have no control over transportation delays, energy failures or communication problems. Financial institutions in the state are not seeking to avoid liability. Rather, they are seeking to eliminate abusive and frivolous suits and claims for punitive damages and to clarify liability for actual damages directly caused by Y2K disruptions. Any limit on claims for damages is conditioned on a financial institution demonstrating good-faith implementation of a Y2K conversion plan.

In addition, one of the major purposes of the bill is to protect the safety and soundness of federally-insured financial institutions by eliminating excessive or punitive damages. The bill contains no caps on actual damages suffered by parties who have a privity of contract with a financial institution. The specific provisions of the bill would be reviewed by the general counsel for NDBA, Marilyn Foss, and I ask your strong consideration for this legislation, which is of major importance to nearly 200 financial institutions in the state with approximately 400 facilities and 8,000 employees.

Banks ready for potential computer bug

By Susan Suda

(Editors note: This is the second of a series dealing with Y2K and how it will affect the area. This week includes visits with area banks to see how they are preparing for the year 2000. Next week we will visit with other businesses in the area.)

REGIONAL—Local bank representatives are assuring customers their finances will all be in order when the year 2000 arrives.

Randy Engesather, assistant vice president at Citizens State Bank in Grafton, said more than a year has been spent so far on dealing with the computer date problem.

"We've gotten our critical systems tested," Engesather said, "which includes our mainframe computer system, links to the Federal Reserve Bank, personal loans and business loans."

He said a copy of live files have been put into a Y2K environment to make transactions using dates of concern. Engesather said manual checks of those transactions were also conducted which indicated all equipment worked correctly.

He added contact has been made with all vendors to make sure they are Y2K compliant.

The next step for Citizen's is to

What is Y2K?

Y2K is a date problem for computers. When computers programmers designed mainframe computers a space saving technique was used to record the date using only the last two digits of the year.

By rewriting a computer's software code, many can be reprogrammed to accept four digits. However, other computers have embedded microchips which must be replaced.

complete how different systems interface or communicate with each other. Since the bank office in Grafton is relatively new and has undergone recent growth, he said much of the equipment and software has already been updated or was Y2K compliant to begin with.

While he is not expecting Jan. 1, 2000, to be a major problem to the consumer or to the bank as an employer, Engesather said the bank has back-up plans in place.

"Even though we have a high degree of confidence, there will be a contingency plan," he said. "We'll still have a what-if or second plan of attack in place even if everything is tested and found to be compliant."

Aware of extensive Y2K plans at other banks, Engesather said consumers should not worry about the banking industry and the new millennium.

"I think the financial industry is the best prepared of any group," he said.

Echoing that sentiment is Cathy Nordquist, vice president of First United Bank in Park River.

"Banks will be very well prepared for the year 2000 because we're so regulated," Nordquist said. "We've already had examiners checking up on our systems."

Nordquist said First United has already completed testing its main system which included running 13 test dates recommended by the FDIC.

She said thus far, approximately \$10,000 in software upgrades, not including man hours, has been spent.

"We've had to replace some software because the companies that made it didn't guarantee its compliance," Nordquist said.

The next phase is to continue running tests with a copy of the bank's data base to ensure transactions will continue to be handled without problems.

Nordquist said she is confident the bank will be able to provide services after Jan. 1, 2000.

"Customers shouldn't be concerned," she said. "Y2K is not new in banking, and we've been calculating into the 2000s for some time

now."

If for some reason power problems occur, Nordquist said First United will be ready.

"We've also done some planning for that," she said. "If there's no power or phone lines are disrupted, we'll still be able to function."

Grafton's Bremer bank president Pete Keeley said an aggressive Y2K plan has already been implemented in the company's tri-state area of North Dakota, South Dakota and Minnesota. Testing of all systems are scheduled to be complete by mid-year.

"By June 30, 1999, we should be 100 percent done," Keeley said. "The only issues we have are the second testing of some systems that we want to run twice."

He said the bank currently runs 78 systems, 16 of which have been designated as "highly critical."

"We're 96 percent done testing on those now," Keeley said.

In addition to software changes or upgrades, Bremer locations will also be undergoing major equipment upgrades including 1,200 new desk top computers throughout the three states. Keeley noted equipment upgrades are not directly Y2K related.

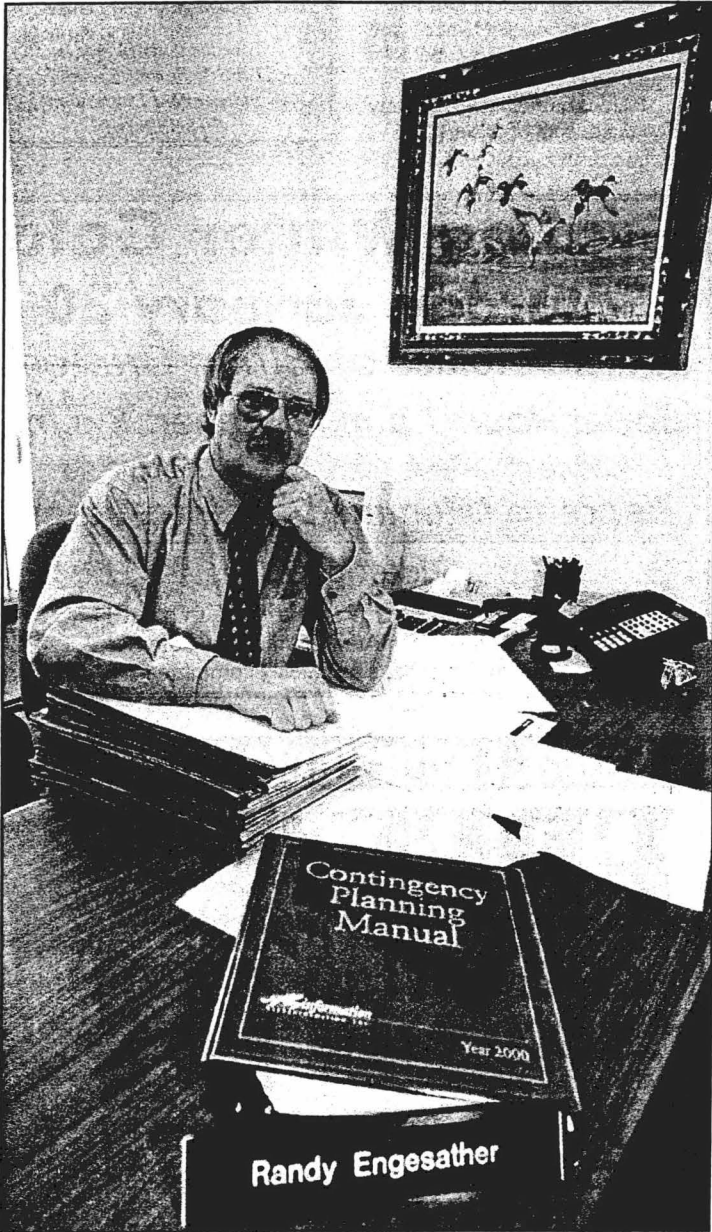
"We're in the process of upgrading equipment in our offices as far as the actual hardware on our desks," he said. "It was time, it's not just Y2K. The process started six months ago and it will be in March when they come to our Grafton office."

Keeley said the cost to Bremer to ensure Y2K compliance, corporation wide, will be in excess of \$500,000, not including the new computers.

He said Bremer's plan also includes contingency plans for "worst-case scenarios."

Like others in the banking industry, Keeley said independent reports indicate banks will be ready for the year 2000.

"The Gartner Group, a well-known firm, has the financial services ranked first in Y2K preparedness," Keeley said. "We've had 30-year mortgages on the books since the '70s and we're confident that Y2K. See page A-10



Area members of the banking industry, including Randy Engesather, assistant vice president at Citizens State Bank in Grafton, are confident financial institutions will be among the most prepared for Y2K. (Photo by Larry Biv)

Y2K: Continued from page A-1

everything will work.”

In addition to ensuring customers that banks will be a “safe harbor for their funds” come Y2K, Bremer is also working to make individual customers aware of how the new millennium will affect them.

“We want them to take a look at their own situations and take inventory of what’s going to work and what won’t,” Keeley said.

Norwest Bank, which recently merged with Wells Fargo & Co., is also in the implementation process of a major Y2K plan. Norwest first began preparing in September 1996 when it opened a Year2000 Project Office. Since Norwest and Wells-Fargo both had established Y2K plans prior to their November 1998 merger, it was decided to continue each separately throughout the year, while sharing best practices to benefit the merger.

According to Ken Loken, president of Grafton’s Norwest location, three of four phases in the company’s plan are substantially complete.

Norwest’s Year2000 Project four phases include:

Phase 1, inventory and assessment, which will identify all date-impacted systems and equipment; establish procedures for modifying and maintaining an inventory; request compliance status and plans from product vendors.

Phase 2, detection, which will identify compliance of date-impacted systems and equipment; identify connections between Norwest and its business partners; set priorities on systems and equipment based on business risk; develop a plan and cost estimate to repair, retire or replace each non-compliant system

and product; establish a testing approach.

Phase 3, remediation, which includes repair, retire or replacement of non-compliant systems and products; prepare detailed testing plans and cost estimate; establish testing organization and environment; conduct unit testing; prepare integration testing plans.

Phase 4, integration testing, which includes conducting internal integration testing; conduct project testing with a representative sample of customers and service providers; augment contingency plans.

Testing at all Norwest sites encompasses everything from vaults to wire transfer systems to elevators.

“What we’re doing now is continuing to work with our customers and having discussions with them about Y2K,” Loken said.

He said this is being done through calls and visits with borrowing customers. Loken stressed the bank is continuing with a business as usual approach for Jan. 1, 2000.

When it comes to the Year 2000...

THERE IS NOTHING SAFER THAN MONEY IN THE BANK

- Banks are consistently rated #1 in Year 2000 preparedness by the Gartner Group and Cap Gemini. (Both are leading and well-known computer industry experts.)
- “The FDIC’s protection of insured deposits will not be affected by the Year 2000.” -- FDIC Chairman Donna Tanoue
- “Your money is safest in the bank. Educate yourself about the Year 2000 situation and what banks are doing to protect consumers,” -- North Dakota Attorney General Heidi Heitkamp.

TESTIMONY SUBMITTED IN FAVOR OF SB 2303

Mr. Chairman, Members of the Committee, good morning. My name is Jim Goetz. I am the President of the Security First Bank of Oliver County in Center, North Dakota, and I serve on the Board of Directors of the Independent Community Banks of North Dakota, and on the Board of Directors of the national Independent Bankers Association of America.

I am here this morning to ask your support for SB 2303, the Year 2000 bank liability bill supported by both the Independent Community Banks of North Dakota and the North Dakota Bankers' Association. My purpose this morning is to provide some background on the Year 2000 initiatives of banking regulators, and on the Year 2000 activities of the banking industry. I would like to start out by saying that no industry has addressed the Year 2000 issue more seriously than the banking industry. Nor has any industry has put more effort in to dealing with the Year 2000 issue or made more progress in dealing with it than the banking industry.

Federal banking regulators have made the Year 2000 issue their absolute number one priority this past year and one half. In my nearly 31 years in the banking industry, I have never seen banking regulators address any issue as aggressively or with such a single minded focus as they have the Year 2000. They have set up strict guidelines and timetables banks must follow and comply with relative to the Year 2000. Each bank was required to draft its own written Year 2000 action plan by June 30, 1998, and that plan had to encompass the following six phases: 1) Awareness; 2) Assessment; 3)

Renovation; 4) Validation; 5) Implementation; and 6) Contingency Planning.

In the first or Awareness Phase, which was to be completed by banks prior to March 31, 1998, banks were required to go through all of their systems and equipment to determine everything that could potentially be affected by a computer chip. Banks were required to review everything from the obvious such as computers and software, to the less obvious such as heating systems, alarms and vaults.

In the second or Assessment Phase, which was to be completed by June 30, 1998, banks were required to inventory all date sensitive systems, processes and procedures, and to begin to determine which were and which were not Year 2000 compliant. They were required to prioritize these systems based upon the criticality of each system. Then banks were required to contact the vendors for each system and to maintain communications files containing periodic status reports from those vendors on the Year 2000 readiness of each of their systems and products. Banks were then required to determine from the vendors that not only were their products ultimately Year 2000 ready, but also, the scope of the vendors' Year 2000 tests, the vendors' definition of Year 2000 compliance, and if a vendor stated they were Year 2000 certified, who certified them and what were the certifying entity's credentials.

The third phase was the Renovation, or "Fixing" Phase, which was to be completed by December 31, 1998. As it implies, during this phase banks were required to have replaced or repaired all systems found not to be Year 2000 ready.

The fourth phase, was the Validation or "Testing" Phase, which was expected to

be well underway by December 31, 1998, and to be completed by March 31, 1999. This is the most time intensive phase and it requires not only the complete testing of each individual system, but also complete testing of the interaction of all of a bank's systems with each other. In addition, testing must not only be conducted for the obvious December 31, 1999 to January 1, 2000 rollover date, but testing must also be conducted on a variety of other dates. Banks must also test (or document why their systems are not affected by) the following ten listed dates: April 9, 1999; September 9, 1999; January 10, 2000; January 31, 2000; February 29, 2000; and March 31, 2000; October 10, 2000; December 31, 2000; January 1, 2001; December 31, 2001.

The fifth phase is the Implementation Phase, which must be completed by June 30, 1999. In this phase, all individual systems used by the bank are certified to be Year 2000 compliant, the bank fully converts to these Year 2000 compliant systems, and the bank's interactive environment finally becomes fully Year 2000 compliant.

The final phase is the Contingency Planning Phase, which should be completed no later than June 30, 1999. This phase requires banks to develop complete contingency plans to cover potential unexpected system failures. These plans must detail how a bank will resume normal business operations if systems do not perform as planned either before or after the century date change. These plans must also address external conditions beyond the bank's control such as power outages.

In addition to the focus on internal systems outlined above, banks have also been required to manage Year 2000 customer risk by contacting all major borrowing and

depositing customers. These contacts must be conducted in detail to ascertain whether or not the bank's major customers have significant Year 2000 risk that could ultimately lead to potential risk for the bank. To give you an idea how comprehensive this customer review is, I have attached a copy of the statement of "Guidance Concerning The Year 2000 Impact on Customers" and its related exhibits which each bank received for implementation from banking regulators. Please note there are pages of questions that banks must answer related to their major customers.

Regulators have also required banks to provide Year 2000 updates to their customers and the general public in an attempt to communicate the bank's progress toward Year 2000 readiness. Banks are also required to attempt to educate the public about the Year 2000 problem in a manner which will avoid any public misinformation and/or lack of confidence.

Furthermore, banking regulators are now requiring banks to develop written Year 2000 liquidity plans. These plans involve calculations of how large potential expected and unexpected year-end customer cash withdrawals might be. And, these plans must detail how the bank will manage its balance sheet to have sufficient liquid assets and currency available to meet those customer withdrawals. And of course these plans must detail the increased security, insurance, etc. that banks must consider depending upon the amount of extra currency they plan to have on hand.

In addition to all of the above, bank regulators are also requiring banks to maintain literally thousands of pages of information documenting the each bank's own

Year 2000 readiness efforts. Everything from notes of conversations with customers on their Year 2000 status to correspondence with banks' suppliers and other business partners must be kept on file.

To insure that banks are on track with their Year 2000 efforts, banking regulators have embarked on the most aggressive bank examination schedule any of us in the industry have ever seen. By the end of this calendar quarter the regulators will have had at least four examination contacts or visits in one year with each bank in the country to ascertain each bank's progress in dealing with the Year 2000. To give you a sense of how comprehensive these examinations are, I have attached a copy of the regulators' Phase Two Year 2000 Examination Work Program as exhibit two.

In addition to their own examinations, bank regulators are also requiring banks to have an independent audits or evaluations of their complete Year 2000 plans, tests, test results and other activities to insure their validity. Furthermore, bank regulators are carefully monitoring the minutes of each bank's Board of Directors minutes to insure that each bank's board is fully aware of the Year 2000 issue, and is fully participating in the bank's Year 2000 remediation process.

It should be noted that banking regulators have also conducted onsite examinations of every bank data processing software vendor, and every bank data processing center in the country with the same rigorous and aggressive standards.

I am proud to be able to relate that recent reports indicate that about 97% of banks in this country have been graded by bank regulators as having made

“satisfactory” progress toward becoming Year 2000 compliant. I would like to note that satisfactory is the highest grade given by the regulators. It should also be pointed out that as of July 31, 1998, only 37 banks out of 10,092 were rated unsatisfactory, and that only one small bank data processing center was rated less than satisfactory. Indeed banking regulators are expressing confidence that the banking industry will be ready for business in the Year 2000 and beyond.

I would also like to note that the bank regulators have effective tools to bring those few banks that have not been rated as satisfactory back on track. Those banks that have had moderate problems in meeting Year 2000 goals and that are rated “needs improvement” may be put under regulatory “memorandums of understanding”, which in layman’s terms mean “you will comply or else.” Those few banks with the most serious problems have undoubtedly been put under regulatory “cease and desist” orders. These orders can go so far as removing even the owners of the bank from the bank’s staff and board of directors, and replacing them with FDIC hand picked management who will cause the bank to become Year 2000 ready.

In our own bank, we, as all other banks, have taken the Year 2000 issue very seriously, not only because of our regulators, but because it just makes good business sense. Our master Year 2000 policy is over 20 pages long and is still growing. Our file containing our Year 2000 supplier and customer contacts, regulatory bulletins, our testing procedures, equipment inventory, etc., has swollen to over 12 inches thick. We have literally checked and tested everything from top to bottom, from our thermostats,

to our telephones, and from personal computers to our mainframe data processing computer. We have spent nearly a five hundred man hours and over \$100,000 testing and replacing questionable equipment with new Year 2000 compliant systems. By the time we complete testing our new systems on March 15, we will have generated over 25,000 pages of computer test printouts validating we are Year 2000 ready.

To be ready for any contingency, we are currently exploring preparing our bank to be able to function for up to six weeks without electrical power. We are making preparations to have enough fuel on hand to be able to travel between our bank, our affiliated bank at New Salem, and the Bank of North Dakota for at least six weeks should normal communications be compromised. We have developed individual contingency plans for each critical item covering everything from computer system failures, to thermostat failures, to the failure of our supplies vendors. We have also developed a master contingency plan which will allow us to process customer transactions manually for an indefinite period of time.

I could go on and on for hours detailing our bank's Year 2000 compliance efforts. But the point is that our bank, along with the other banks in the nation, is doing everything imaginable and humanly possible to insure that our customers will receive uninterrupted banking services before and after the turn of the century.

Mr. Chairman, Members of the Committee, I would submit that there is no doubt that banks are going far above and beyond all other industries in preparing for the Year 2000. Banks and banking regulators are doing absolutely everything within their power

to make sure that banks and their customers do not have Year 2000 problems.

I would also submit that there is no more highly regulated industry in the nation than banking. And, as you are aware, that intense regulation brings tremendous costs and other burdens to the banking industry that are not shared by other industries. I would suggest that because of that tremendous regulatory burden, and because of the huge amounts of expense and effort the banking industry has invested in the Year 2000, that the banking industry has already paid its Year 2000 dues. As such the banking industry is in a unique niche, and fully deserves the measure of potential relief SB 2303 will provide.

I would also like to note that this bill not will hurt bank customers, this bill will only serve to protect banks from having to defend against frivolous lawsuits, related to events such as prolonged power or telecommunications outages, shortages of US currency and the like.

In closing, Mr. Chairman and Members of the Committee, please vote for fairness for North Dakota's community banks.

PLEASE VOTE "DO PASS" ON SB 2303.

Thank you.

JIM GOETZ

EXHIBIT 1

FFIEC Letterhead - March 17, 1998

**GUIDANCE CONCERNING
THE YEAR 2000 IMPACT ON CUSTOMERS**

To: The Boards of Directors and Chief Executive Officers of all federally supervised financial institutions, Department and Division Heads of each FFIEC agency, and all examining personnel.

BACKGROUND

The Federal Financial Institutions Examination Council (FFIEC) has issued three statements providing guidance on the Year 2000 problem. Two interagency statements were issued in June 1996 and May 1997 to address the key phases of the Year 2000 project management process. The most recent guidance, published in December 1997, outlined the specific responsibilities of senior management and the board of directors to address risks associated with the Year 2000 problem.

PURPOSE

The purpose of this guidance is to assist financial institutions in developing prudent risk controls to manage the Year 2000-related risks posed by their customers. This guidance describes a variety of approaches for a financial institution's senior management and board of directors to assess the risks arising from the failure or inability of the institution's customers to address their Year 2000 vulnerabilities. This guidance outlines the due diligence process that financial institutions should adopt to manage their Year 2000-related risks arising from relationships with three broad categories of customers: funds takers, funds providers, and capital market/asset management counterparties.

SUMMARY

Key points addressed in this guidance include:

- A financial institution can face increased credit, liquidity, or counterparty trading risk when its customers encounter Year 2000-related problems. These problems may result from the failure of a customer to properly remediate its own systems and from Year 2000 problems that are not addressed by the customer's suppliers and clients. By June 30, 1998, senior management should have implemented a due diligence process which identifies, assesses and establishes controls for the Year 2000 risk posed by customers. By September 30, 1998, the assessment of individual customers' Year 2000 preparedness and the impact on an institution should be substantially completed.

- The due diligence process outlined in this guidance focuses on assessing and evaluating the efforts of an institution's customers to remediate their Year 2000 problems. Year 2000 issues related to the institution exchanging data with its customers should be addressed as a part of the institution's internal Year 2000 project management program.
- The guidance recognizes that each institution must tailor its risk management process to its size, its culture and risk appetite, the complexity of its customers, and its overall Year 2000 risk exposure. The FFIEC understands that these differences will affect the risk management programs developed by financial institutions. However, financial institutions must evaluate, monitor, and control Year 2000-related risks posed by funds providers, funds takers, and capital market/asset management counterparties.
- The institution's due diligence process should identify all customers representing material Year 2000-related risk, evaluate their Year 2000 preparedness, assess the aggregate Year 2000 customer risk to the institution, and develop appropriate risk controls to manage and mitigate Year 2000 customer risk.
- Risk management procedures will differ based on a variety of factors, including the institution's size, risk appetite and culture, the complexity of customers' information and operating systems, and the level of its own Year 2000 risk exposure. The Year 2000 due diligence processes used by smaller institutions may not be as extensive or formal as those in larger institutions where customers may be more dependent upon information technology.
- The attached appendices provide examples of processes used by financial institutions to manage Year 2000-related customer risk.
- An institution's management should provide quarterly reports to the board of directors that identify material customers who are not effectively addressing Year 2000 problems. The reports should summarize the action taken to manage the resulting risk.

OVERVIEW

The Year 2000 problem presents many challenges for financial institutions and their customers. The FFIEC recognizes that risk management procedures will vary depending on the institution's size, its risk appetite and culture, the complexity of customers' information and operating systems, and the level of its own Year 2000 risk exposure. For example, customers of small community financial institutions may not depend on computer-based information systems to the same extent as large business customers of large financial institutions. As a result, Year 2000 due diligence processes used by these institutions may not be as extensive or formal as those in institutions whose customers may be more dependent upon information technology. Senior management should oversee the development and implementation of a due diligence process which is tailored to reflect the Year 2000 risk in their institution's customer base.

Three major types of customers may expose a financial institution to Year 2000-related risks. They include funds takers, funds providers, and capital market/asset management counterparties.

- **Funds Takers**
Funds takers include borrowers and bond issuers that borrow or use bank funds. Failure of fund takers to address Year 2000 problems may increase credit risk to a financial institution through the inability of fund takers to repay their obligations.
- **Funds Providers**
Funds providers provide deposits or other sources of funds to a financial institution. Liquidity risk may result if a funds provider experiences a Year 2000-related business disruption or operational failure and is unable to provide funds or fulfill funding commitments to an institution.
- **Capital Market/Asset Management Counterparties**
Capital market and asset management counterparties include customers who are active in domestic and global financial markets. Market trading, treasury operations, and fiduciary activities may be adversely affected if a financial institution's capital market and asset management counterparties are unable to settle transactions due to operational problems caused by the Year 2000 date change.

GENERAL RISK CONTROL GUIDELINES

By June 30, 1998, financial institutions should establish a process to manage the Year 2000 risks posed by its customers. The process should: (1) identify material customers; (2) evaluate their Year 2000 preparedness; (3) assess their Year 2000 risk to the institution; and (4) implement appropriate controls to manage and mitigate their Year 2000-related risk to the institution. The assessment of individual customers' Year 2000 risk and their impact on an institution should be substantially completed by September 30, 1998. Year 2000 issues related to data exchanges between the institution and customers should be addressed as a part of an institution's internal Year 2000 project management program.

- **Identify Material Customers**
Management should identify customers that represent material risk exposure to the institution, including international customers. Material risk exposure may depend on:
 - ▶ Size of the overall relationship;
 - ▶ Risk rating of the borrower;
 - ▶ Complexity of the borrower's operating and information technology systems;
 - ▶ Customer's reliance on technology for successful business operations;
 - ▶ Collateral exposure for borrowers;
 - ▶ Funding volume or credit sensitivity of funds providers; and

- ▶ Customer's dependence on third party providers of data processing services or products.

- **Assess Preparedness of Material Customers**

The impact of Year 2000 issues on customers will differ widely. Smaller financial institutions may find that most of their material borrowers use either manual systems or depend on commercial software products and services. The evaluation of Year 2000 preparedness for these customers will be less involved and may not require additional risk management oversight. To ensure consistent information and a basis for comparisons among customers, management should address the following.

- ▶ Train account officers to perform a basic assessment of Year 2000 risk of customers.
- ▶ Develop a standard set of questions to assess the extent of a customer's Year 2000 efforts. Appendices A - D contain samples of forms some financial institutions use to evaluate customer Year 2000 preparedness. Financial Institutions are not required to use these forms, although they provide useful examples of methods to evaluate customer preparedness.
- ▶ Update the status of a customer's Year 2000 efforts periodically, but at least semi-annually. For customers that represent significant Year 2000 exposure to the institution, quarterly updates may be necessary.
- ▶ Document Year 2000 assessment conclusions, subsequent discussions, and status updates in the institution's customer files.

- **Evaluate Year 2000 Risk to the Institution**

After identifying all customers representing material Year 2000 risk and evaluating the adequacy of their Year 2000 programs, management should assess the Year 2000 risk posed to the institution by these customers, individually and collectively. Management should determine whether the level of risk exposure is high, medium, or low.

Management also should provide quarterly updates to the board of directors on customers that are not addressing Year 2000 problems effectively and discuss the actions taken by the institution to control the risk.

- **Develop Appropriate Risk Controls**

Once the institution has evaluated the magnitude of Year 2000 risk from its customers, management must develop and implement appropriate controls to manage and mitigate the risk. Senior management should be active in developing risk mitigating strategies and ensure that effective procedures are implemented on a timely basis to control risk.

SPECIFIC RISK CONTROL GUIDELINES

The specific risk controls an institution implements will vary depending on the size of the institution, its risk appetite and culture, the complexity of customers' information and operating

systems, and its own level of Year 2000 risk exposure. Different risk management controls may be needed to address unique and material Year 2000 issues that arise from business dealings with different categories of customer.

- **Funds Takers**

An institution's Year 2000 risk management controls for funds takers should focus on limiting potential credit risk by ensuring that Year 2000 problems do not prevent a borrower or bond issuer from meeting the terms of its agreements with the institution. Controls to manage an institution's exposure to its funds takers should address underwriting, documentation, credit administration, and the allowance for loan and lease losses (ALLL). These same factors also should be considered, where appropriate, when evaluating risk posed by an institution's capital market and asset management counterparties.

- ▶ **Underwriting**

During any underwriting process, management should evaluate the extent of the borrower's Year 2000 risk. Specifically, management should:

- Ensure that underwriters are properly trained and have sufficient knowledge to perform a basic assessment of Year 2000 customer risk. There are a number of resource materials available that will assist in informing lenders of Year 2000 issues. State and national trade associations have prepared materials to assist lenders understand customer risk created by the Year 2000. Additional information is available on the Internet and can be located by searching on the words "Year 2000".
- Evaluate whether Year 2000 issues will materially affect the customer's cash flows, balance sheet, or supporting collateral values. As a part of the assessment and based on materiality, management should consider the complexity of the customer's operations; their dependence on service providers or software vendors; the extent of management oversight of the Year 2000 project; the resources the customer has committed to the project; and the date the customer expects to complete Year 2000 efforts.
- Control credit maturities or obtain additional collateral, as appropriate, if credit funding is to be continued for high-risk customers.

- ▶ **Documentation**

Proper loan documentation provides an effective means to monitor and manage the Year 2000 risk posed by borrowers. Loan documents should reflect the degree of risk posed by customers. Institutions should consider incorporating some or all of the following into loan agreements:

- Representations by borrowers that Year 2000 programs are in place;
- Representations that borrowers will disclose Year 2000 plans to the lender, provide periodic updates on the borrower's progress of the Year 2000 program, and provide any assessment of the borrower's Year 2000 efforts conducted by a third party; and
- Audits that address Year 2000 issues.
- Warranties that the borrower will complete the plan;
- Covenants ensuring that adequate resources are committed to complete the Year 2000 plan; and
- Default provisions allowing the lender to accelerate the maturity of the debt for non-compliance with Year 2000 covenants;

▶ **Credit Administration**

After the initial assessment, ongoing credit administration provides the best opportunity for an institution to manage Year 2000-related customer risk. Periodic credit analyses, which should include an update of the customer's Year 2000 efforts, can help to monitor a borrower's Year 2000 efforts. When performing credit analyses, loan officers should determine whether a customer's Year 2000-related risk merits an adjustment to its internal risk rating.

▶ **ALLL Analysis**

Management's review of the adequacy of loan and lease loss allowances should include Year 2000 customer risk. When Year 2000 issues adversely impact a customer's creditworthiness, the allowance for loan and lease losses should be adjusted to reflect adequately the increased credit risk. Additionally, management's analysis of loss inherent in the entire portfolio should reflect Year 2000 risk.

• **Funds Providers**

Management should consider the potential effect on an institution's liquidity by assessing the potential for unplanned reductions in the availability of funds from significant funding sources that have not taken appropriate measure to manage their own Year 2000 problems. Management should develop appropriate strategies and contingency plans to deal with this potential problem.

▶ **Risk Assessment of Funds Providers**

As with funds takers, management should discuss Year 2000 issues with significant funds providers, evaluate their Year 2000 readiness to the extent possible, and assess the Year 2000-related risks posed by the providers. Management should be aware of concentrations -- including concentrations in any single currency -- from an individual provider or group of providers that may not be Year 2000 ready.

▶ **Contingency Planning**

The risk assessment of major funds providers' Year 2000 readiness should be incorporated into an institution's liquidity contingency plans. As with other contingency planning processes, management should evaluate its exposure and potential funds needs under several scenarios that incorporate different assumptions about the timing or magnitude of funds providers' Year 2000-related problems. Institutions with significant funds flows in different currencies may need separate contingency plans for each major currency.

Although the liquidity risks from funds providers' Year 2000-related problems are similar to other "event risks" that institutions address in their liquidity contingency plans, Year 2000-related liquidity risks differ because the date of this event is known in advance. As a result, institutions may be better able to plan for and mitigate potential liquidity risks. For example, institutions may be able to reduce potential liquidity risks by extending the maturity of their advances under funding lines sufficiently past January 1, 2000, to provide time to assess and evaluate the effect of the Year 2000 on its funds providers. Maintaining close contact with funding sources throughout this potentially difficult period can provide management with timely, market sensitive information and thus allow for more effective liquidity planning.

- **Capital Market and Asset Management Counterparties**

The focus of the controls for an institution's exposure to Year 2000-related problems in capital markets and among counterparties mirror those needed for funds takers and funds providers. Potential Year 2000-related problems with capital market participants range from a counterparty's failure to complete a securities transaction or derivatives contract settlement to, in extreme cases, the failure of the counterparty itself. A counterparty failure could lead to the total loss of the value of the payment or contract. A counterparty's failure to settle a transaction could cause the institution unexpected liquidity problems, which in turn could result in the failure of a financial institution to deliver dollars or foreign currencies to its counterparties.

In addition, Year 2000-related problems among fiduciary counterparties could prevent a financial institution from fulfilling its fiduciary responsibilities to protect and manage assets for fiduciary beneficiaries. A counterparty's failure to remit bond payments, fund employer pension contributions or settle securities transactions could increase the institution's fiduciary risk.

- ▶ **Risk Assessment of Counterparties**

As part of a sound due diligence process, management should identify and discuss Year 2000 compliance issues with those counterparties which represent large exposures to the bank itself and to fiduciary account beneficiaries. Financial institutions should evaluate counterparty exposure and develop risk reducing action plans to help manage and control that risk.

Risk Reduction Plans

In cases where institutions are not fully satisfied that their counterparties will be Year 2000 ready, management should establish mitigating controls such as early termination agreements, additional collateral, netting arrangements, and third-party payment arrangements or guarantees. In cases where management has a high degree of uncertainty regarding a counterparty's ability to address its Year 2000 problems, the institution should consider avoiding transactions with settlement risk after January 1, 2000. As noted earlier, the interest rate effect of material mismatches of funding, or maturity, should be evaluated as maturity and settlement risk is adjusted. The financial institution should not resume normal transaction activities until the counterparty has demonstrated that it will be prepared for the Year 2000.

CONCLUSION

Financial institutions face significant internal and external challenges from Year 2000-related risks posed by their customers. The concepts and guidance in this interagency statement are designed to assist institutions in developing appropriate risk controls. The FFIEC recognizes that risk management procedures may vary depending on the institution's size, its risk appetite and culture, the complexity of its customers' information systems, and its own Year 2000 risk exposure. While these differences will affect the risk management practices developed by management, it is essential that financial institutions identify, measure, monitor and control Year 2000-related risks posed by funds providers, funds takers, and capital market/asset management counterparties.

Appendices (4)

Appendix A

YEAR 2000 QUESTIONNAIRE

FOR CUSTOMERS OF _____ BANK

Customer Name: _____ Date: _____

Relationship Manager: _____

Please complete the questionnaire based on responses from the customer. If necessary, comment in the space provided or attach additional information to this form. Any "No" answers require appropriate follow-up with the customer on a periodic basis. Please retain a copy of this form in the credit file.

	Yes	No	N/A
1. Has the company developed a comprehensive plan for Year 2000 compliance?			
2. Is someone in the company specifically responsible for managing the Year 2000 plan?			
3. Has senior management and the board of directors reviewed and approved the plan?			
4. Has the company completely inventoried its software, hardware, and telecommunications?			
5. Has the company identified all equipment with date-sensitive operating controls such as elevators, HVAC, security systems, manufacturing equipment, etc.?			
6. Has the company verified that vendor-supplied systems will be Year 2000 compliant?			
7. Has the company verified Year 2000 compliance of outside data-processing companies and established a testing time frame?			
8. Has the company budgeted sufficient resources (both financial and personnel) to accomplish its Year 2000 mission?			

Has the plan been reviewed by the company's outside auditors?			
10. Does the company's plan call for remediation and preliminary testing of critical systems to be largely completed by 12/31/98?			
11. Will the company have contingency plans for mission critical systems in place by 12/31/98?			
12. Does the company have any ongoing or long-term contracts that could subject it to liability if it failed to perform as a result of Year 2000 compliance failure?			
13. Has the company discussed potential legal ramifications or expenses with its attorney?			
14. Has the company discussed potential losses from Year 2000 problems with insurers to determine coverage of any losses?			

Comments:

Appendix B

YEAR 2000 WORKSHEET

The following are issues surrounding Year 2000 that your relationship manager will be discussing with you in the near future. Please note that this worksheet should not be used and is not intended to be used by you to determine whether your company needs to enlist assistance in assessing and addressing your company's Year 2000 preparedness and/or exposure. For answers and assistance regarding Year 2000 questions, you should contact qualified professionals of your choice.

Circle Response	ISSUE IDENTIFICATION
Y N N/A	• Has your company begun its assessment of the scope of being Year 2000 compliant?
Y N N/A	• Are your following systems capable and ready to handle Year 2000 processing?
Y N N/A	• Information processing (hardware and software)
Y N N/A	• Delivery (telecommunication and transportation)
Y N N/A	• Manufacturing (robotics, lighting, heat, water supplies)
Y N N/A	• Real estate (HVAC, security, card access, elevators)
Y N N/A	• Support (insurance, license, automatic inventory control)
Y	• For each "No" answer to the last question, which systems need to be modified to handle year 2000 processing?
Y	• Information processing
Y	• Delivery
Y	• Manufacturing
Y	• Real estate
Y	• Support
Y N N/A	• Has any vendor of any of the above advised that they will not make their system Year 2000 compliant? Please specify.
Y N N/A	• If outside data processing service bureaus are used, have they been verified for Year 2000 compliance and a testing time frame established?
Y N N/A	• Do you have any ongoing or long term contracts that could subject you to liability if you failed to perform as a result of a Year 2000 compliance failure?
	SPONSORSHIP/MONITORING
Y N N/A	• Has your company assigned overall responsibility for the Year 2000 effort to a senior manager?
Y N N/A	• Does the process include regular reporting to and monitoring by senior management?
Y N N/A	• Does the process include regular reporting to and monitoring by the Board?

OVERALL PLAN

• Does your company have a Year 2000 problem resolution process that includes:

• Has your company discussed a Year 2000 problem resolution process that includes (Awareness, assessment, renovation, etc.):

Y N N/A
 Y N N/A
 Y N N/A
 Y N N/A
 Y N N/A
 Y N N/A

- Awareness of the problem
- Inventory check list*
- Assessment of complexity
- Remediation
- Validation/Testing
- Implementation

With Key Suppliers

With Key Customers

Yes	No	N/A	Yes	No	N/A
Yes	No	N/A	Yes	No	N/A
Yes	No	N/A	Yes	No	N/A
Yes	No	N/A	Yes	No	N/A
Yes	No	N/A	Yes	No	N/A
Yes	No	N/A	Yes	No	N/A

*Complete list of equipment, software, etc., that may be affected by the Year 2000 issue

Y N N/A

• Has your company discussed the Year 2000 issue with its major suppliers, service providers or customers in terms of any system interfaces that may exist between them?

RESOURCE ISSUES

Y N N/A
 Y N N/A
 Y N N/A
 Y N N/A

- Has your company established a budget for the Year 2000 effort (determined how much and how the expenditures will be financed)?
- Has your company assigned adequate personnel resources to the project?
- Has your company discussed potential legal ramifications or expenses with its attorney?
- Will your company's CPA firm help in this task?
- Has your company hired a consultant to assist with Year 2000 issues?

TIMING

Y N N/A

- Has your company established project target dates and deliverables for the Year 2000 effort?
- By what date does your company's Year 2000 plan call for the renovation and testing of all mission critical systems to be largely completed? Date _____
- By what date will contingency plans for mission critical systems be in place? Date _____

Year 2000
Customer Evaluation

Customer Name: _____
Obligor #: _____

Rel Mgr/Mail Code: _____
Date: _____

Instructions: Complete the evaluation based on responses to the Customer Questionnaire, Customers rated "High" or "Medium" require quarterly follow-up until their "Status" is rated "1". Forward a copy of completed forms to Loan Administration. Retain a copy of this form in the Credit File.

1. Rate the company's sensitivity to Year 2000 risk based on the following information about the company's operations:

High Medium Low (circle one)

High

- a. Could not conduct its business
If it did not have computers, or
- b. Operates in computer-related
industry, or
- c. Has major customers, suppliers,
or vendors which meet (a) or (b)
above.

Medium

- a. Computers only used in
financial, accounting, and
recordkeeping functions, or
- b. Has customers or suppliers
that are systems impacted

Low

- a. Minimal reliance on
computers to conduct its
business

2. Rate the status of the company's Year 2000 implementation on the following scale (1-6, with 1 representing most progress to 6 representing least progress):

1 2 3 4 5 6
(circle one)

- 1. Has Year 2000 plan with budget, implementation dates in place
 - Plan has senior management (and Board) support and regular reporting on status.
 - Plan is evidenced by material progress toward testing and implementation
 - Year 2000 issues have been discussed with information system vendors, key customers, and suppliers
- 2. Has Year 2000 plan with budget, implementation dates in place
 - Limited action taken on plan implementation to date
- 3. Has preliminary Year 2000 plan and budget drafted but not finalized and approved
 - Very limited or no action taken to date
- 4. Aware of Year 2000 issue and intends to draft a plan but has not begun
- 5. Not fully aware of Year 2000 issue
- 6. No intention of completing a Year 2000 plan

Appendix C

Millennium Risk Evaluation

Yes No

I. Awareness

A. Is the customer realistically aware of and does the customer understand the Year 2000 or Millennium problem and the potential business and financial risks to which he or she is exposed?

Yes No

A. Does the customer fully understand how their industry, business, customers and key partners can be affected? Different industries are impacted in very different ways. A casual explanation is probably a warning that the issue has not been explored in depth. A quick glance at the millennium matrix can guide you to complexity levels.

B. Has the customer identified an individual and/or a working group responsible for all functions impacted by Year 2000?

Yes No

B. If an individual has not been selected to lead the program, then a program does not exist. Identify the person. Is this a full time job? Are their skill sets consistent with the task?

Name: _____

C. Is the customer relying on:

internal external resources?

C. Reliance on third parties is not uncommon, but heavy use of external resources can increase the risk by not having full control at all times.

II. Vulnerability and Dependency

A. Are mainframe or minicomputer applications critical to core business operation, whether in-house or outsourced?

Yes No

A.B.C. It is hard to imagine industries where computers are not critical, functions/operation are not automated, or where critical dependencies do not exist; we are seeking high levels of criticality where alternatives are few and the business functionality is at risk. These questions could be answered through a relationship manager's own knowledge of the business/industry.

B. Does the core business operation depend on automated processes, whether delivered on desktop computers or mainframes, whether in-house or outsourced?

Yes No

C. Do critical dependencies exist (suppliers, customers) that are vulnerable to Year 2000 disruptions?

Yes No

III. Assessment

A. Has the customer performed an assessment of the Year 2000 impact on its system and business operations?

Yes No

A. An assessment is the foundation of serious planning and budgeting. The discussion should cover major business segments; for example, inquiring how major balance sheet categories could be negatively impacted by incorrect date calculations could form the basis of determining how deeply the customer has analyzed its condition. Lack of an assessment is a red flag.

B. Has the customer developed a complete inventory of all hardware (including mainframes, minicomputers, local and wide area networks and personal computers), firmware, and software (including systems and applications) components for all EDP systems?

Yes No

B. The inventory of hardware, firmware, and software falls out of the assessment and vice versa. If the inventory has not been taken, than a plan and budget cannot be completed. The entire program is suspect.

C. Has the customer had to provide certifications or disclose millennium status to third parties?

Yes No

C. Ask about the nature and frequency of inquiries being directed at the borrower, which will mirror the nature of their issues and industry challenges. Can you see a few? Do they keep a log?

Current Status

Yes No

A. At what stage is the customer in his or her Year 2000 project:

- Has not started
- Up to 1/4 complete
- Up to 1/2 complete
- Up to 3/4 complete
- More than 3/4 complete

A. B. C. Keep in mind that there is a date certain by which this work must be done; it cannot be moved. In discussing the date of completion and the status thereof, determine how much reliance has been placed on third party delivery dates, which are outside of company control.

D. Testing is critical to ensure trouble-free operations.

B. Does the customer report that he or she is on schedule?

Yes No

C. Does the customer report that the project will be completed before Year 2000?

Yes No

D. Will there be time for testing?

Yes No

V. Budget, Planning and Impact

A. Has the customer developed a credible plan and budget for the Year 2000 project that is properly funded?

1. What is the estimated cost? \$ _____
2. Millennium cost as a % of Technology budget? \$ _____
3. Expended to date? \$ _____
4. Over how many years spent? \$ _____

A. After some discussion on resources, inventory, pervasiveness of technology; etc., you should be developing an opinion on whether the plan and budget, if they exist, are indeed appropriate and credible. We do not expect you to be technology experts, but reasonably informed on your customers' efforts to remediate their systems.

B. We are asking you to consider the impact of failure to remediate systems. Is capacity to pay impacted in a way that will affect a risk rating?

B. What is the impact to the customer if Year 2000 issues and programs are not successfully completed?

- No downgrade, or downgrade within pass categories Green
- Downgrade to problem loan status Yellow
- Risk of loss Red

C. Consider this question in the light of the specificity of the plan, the complexity of the operations, the resources and funds dedicated to the project, and the track record of management in overcoming similar challenges. In situations where risk of loss or downgrade to problem loan status is the outcome of failure, we need to be very certain of the answer.

C. In your opinion, will this customer meet significant Year 2000 timetables?

- Highly likely Green
- Tight schedule - not sure Yellow
- Unlikely Red

Appendix D

Appendix D

Year 2000: Credit Risk Assessment Worksheet

Y2K Credit Risk Assessment Worksheet Page 1

Information

The purpose of this worksheet is to help credit officers assess the level of a business borrower's risk associated with the Year 2000 (Y2K) problem and to ensure consistency of Y2K risk assessment approach.

The worksheet is multidimensional, assessing (1) the borrower's overall vulnerability to the Y2K problem, (2) the borrower's resources to manage the problem, and (3) the adequacy of the borrower's Y2K plan.

Although designed in a "check-the-box" format, the worksheet does not replace thoughtful and informed analysis.

Add to this worksheet issues that are specific to the business that you are assessing. Record and support appropriate conclusions driven by your information and analysis, whether or not derived directly from the worksheet logic.

The worksheet is divided into four parts:

- Part 1 is an overall Y2K *credit risk* conclusion, based on the assessments in Parts 2, 3, and 4.
 - Part 2 is a *vulnerability* assessment, which helps to determine whether the business because of its reliance on technology, supplier, and or customer concentrations, and other considerations is at high, medium, or low risk to the Y2K problem.
 - Part 3 is a *financial, management, and technology resource* assessment, which helps to determine whether the business is at high, medium, or low risk in relation to the depth and stability of resources available to address its Y2K problem.
 - Part 4 is a Y2K *plan* assessment, which helps to determine whether the business is at high, medium, or low risk based on the adequacy of its Y2K plan.
-

Borrower Name _____	Risk Rating _____
Borrower Industry _____	SIC _____
Binding Commitments (\$000) _____	
Worksheet Prepared by _____	Telephone _____
Unit Name _____	Unit # _____
Date Prepared _____	

Part 1: Year 2000 Credit Risk Summary and Conclusion

Complete Part 1 after completing Parts 2, 3, and 4 on the following pages. Section C is provided for updating conclusions at intervals as required by managers or as new information is obtained from the borrower.

A: Summary of Conclusions from Parts 2, 3, and 4			
Part 2. Y2K Vulnerability Risk	<input type="checkbox"/> Low	<input type="checkbox"/> Medium	<input type="checkbox"/> High
Part 3. Y2K Resource Risk	<input type="checkbox"/> Low	<input type="checkbox"/> Medium	<input type="checkbox"/> High
Part 4. Y2K Plan Risk	<input type="checkbox"/> Low	<input type="checkbox"/> Medium	<input type="checkbox"/> High

B: Conclusion: Overall Y2K Credit Risk Assessment

Based on the above and other considerations as applicable, determine an overall Y2K credit risk conclusion for the borrower. Generally, if both resource and vulnerability risk assessments are low, the conclusion should be low overall risk regardless of the adequacy of the Y2K plan.

Low Y2K credit risk

Medium Y2K credit risk

High Y2K credit risk

Comments:

C: Update

Date: _____ Name (if differs from above): _____ BANet: _____

Based on information in the comments below, provide an updated Y2K credit risk conclusion.

Low Y2K credit risk

Medium Y2K credit risk

High Y2K credit risk

Comments:

Part 2. Year 2000 Vulnerability Assessment			
A. Overall technological and business vulnerability to the year 2000 problem			
	Yes	No	Comments
Are mainframe or mini-computer applications critical to core business operation, whether in-house or outsourced?			
Does core business operation depend on one or more automated processes (e.g., inventory, assembly line, shipping, customer orders, etc.), whether delivered on desktop computers or mainframes, whether in-house or outsourced?			
Does the business depend on any one supplier for 25% or more of inventory, is there a single mission critical supplier, and/or is the supply chain generally vulnerable to Y2K disruption?			
Does the business depend on any one customer for 25% or more of revenue and/or is the customer base generally vulnerable to Y2K disruption?			
Are there other key Y2K vulnerabilities? If you check yes, explain your assessment in the comment section.			
B. Vulnerability Risk Conclusion			
<ul style="list-style-type: none"> If all boxes in Section A. Above are checked No, it is likely that business vulnerability risk is low; if this is your conclusion, stop here and indicate low vulnerability risk below. If one or more boxes above have been checked Yes, vulnerability to the Y2K problem is medium to high. Continue Part 2 by checking <i>yes</i> or <i>no</i> to the following (substantiate all <i>yes</i> responses). 			
	Yes	No	Comment/Substantiation of "Yes" Response
Is the business by its nature generally not vulnerable to technology failure (e.g., some personal service businesses)?			
If there is a business interruption caused by a Y2K problem, could the business recover rapidly because of ready accessibility of viable alternatives, or other reasons particular to this business operation?			
<ul style="list-style-type: none"> If one or more of the section B boxes above are checked Yes, it is likely that Y2K vulnerability is medium; if this is your conclusion, indicate medium vulnerability risk below. If both boxes are checked No, it is likely that Y2K vulnerability is high; if this is your conclusion, indicate high vulnerability risk below. 			
Overall Year 2000 Vulnerability Conclusion			
Technological and business vulnerability risk is: <input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High		Comments:	

Part 3. Year 2000 Resource Risk: Financial, Management, and Technological Assessment

Consider the adequacy of financial, management, and technology resources in relation to the extent of the technological vulnerability risk identified in Part 1.

Low Resource Risk

Financial, management, and technology resources (whether in-house or outsourced) available to address Y2K are superior to exceptional and business is not facing other unavoidable internal or external challenges likely to divert necessary resources.

Medium Resource Risk

Financial resources available to address Y2K are ample, management quality is good, technological expertise is readily available (in-house or outsourced) and business is not facing other unavoidable internal or external challenges likely to divert necessary resources.

High Resource Risk

Financial resources available to address Y2K are marginal to inadequate, management depth is thin, technological expertise is marginal to inadequate or not readily available, and/or business is facing other unavoidable claims on cash flow or business stability that threaten the adequacy of resources available for Y2K.

Comments:

Part 4. Year 2000 Plan Assessment (based on discussions with management).

	Yes	No	N/A	Comments
Does the business have a comprehensive Y2K plan that effectively prioritizes mission-critical systems?				
Does the Y2K plan have the endorsement and involvement of executive management?				
Has management clearly established that implementation of the Y2K plan has first priority?				
Does the Y2K plan include vendor compliance?				
Does the Y2K plan include contingencies for the impact of Y2K business interruptions affecting key vendors, suppliers, or customers?				

Part 4. Year 2000 Plan Assessment Continued

	Yes	No	N/A	Comments
Does the Y2K plan include computer controlled systems such as telecommunications, security systems, elevators, and climate control?				
Has a Y2K budget been established? (Enter budget totals in Comments.)				(\$000) 1997 \$ _____ 1998 \$ _____ 1999 \$ _____ 2000 and beyond \$ _____
Has the business incorporated the effect of Y2K into its financial planning?				
Has the business taken any steps to ensure key staff do not leave prior to project completion?				
Is the business generally meeting its plan deliverables at the dates specified in the plan?				Target completion date _____
Is the business developing contingency plans to mitigate risk if the Y2K project is not completed on time?				
Other key considerations:				

Overall Plan Assessment

<input type="checkbox"/> Low Risk: Good Overall Plan All questions above are answered yes or not applicable	<input type="checkbox"/> Medium Risk: Adequate Plan Most questions above are answered yes or not applicable; those that are answered no are not critical to success.	<input type="checkbox"/> High Risk: Inadequate Plan Most questions above are answered no, or one or more answered no are critical to success.
---	--	---



YEAR 2000

WORKPROGRAM

PHASE II

VERSION 3.02

Number:

Institution/Organization Name:

City/State:

Date of Review:

Examiner In-Charge:

INTRODUCTION

The following examination procedures are for use in federally supervised financial institutions, service providers, and software vendors. The examination procedures will help the examiner to determine if the institution has addressed the Year 2000 problems inherent in many computer software, hardware, and environmental systems as well as indirect risks associated with external sources, customers, or fiduciary activities. The examination procedures are designed to focus on the adequacy of the institution's plans and processes for achieving Year 2000 readiness, with particular emphasis placed on the final phases of the Year 2000 project. These procedures apply to systems in domestic institutions and in their foreign branches and subsidiaries.

GENERAL INSTRUCTIONS

The workprogram is divided into six sections (General, Renovation, Validation, Implementation, Contingency Planning, and Examination Conclusions), each containing a series of work steps and related examination procedures. In most cases, related examination procedures are then subdivided in categories for general procedures, serviced institutions, turnkey institutions, and large or complex organizations. The subdivided categories are defined below.

General Procedures	These procedures should be performed, as applicable, during all reviews of financial institutions, service providers, or software vendors.
Serviced Institutions	Procedures detailed under the subheading of "Serviced Institutions" should be performed, as applicable, during reviews of institutions in which mission-critical data processing services are provided by an affiliated or nonaffiliated data processing service provider.
Turnkey Institutions	Procedures under this subheading should be performed, as applicable, during reviews of institutions which rely on outside vendors for mission-critical hardware and software.
Large or Complex Organizations	Procedures under the subheading of "Large or Complex Organizations" should be performed, as applicable, if the review is being conducted at any one of the following: an independent service provider, a financial institution or a subsidiary of a holding company which services other financial institutions, a software vendor, a financial institution which does in-house programming, a financial institution with total assets greater than \$1 billion, and a financial institution whose systems are deemed complex.

For certain hybrid institutions, such as those which exhibit a blend of turnkey and serviced characteristics, examiners would use an appropriate blend of questions under the serviced institution and turnkey institution headings.

This workprogram provides a risk-focused approach to the Year 2000 on-site examination process. Therefore, an examination seldom will require every step in the workprogram to be performed. Examiners should complete those worksteps and examination procedures which are necessary to respond to the requirements in the Examination Conclusions Section. The scope of the

examination should be appropriate to the nature and sophistication of the entity under review; institution management's understanding of the Year 2000 issue and their ability to oversee the institution's Year 2000 correction process; and to the institution's current progress in completing its Year 2000 project phases. Examiners may leverage the efforts of internal/external audit when this work is deemed effective in evaluating the entity's Year 2000 readiness. Note that not all institutions, or all systems within an institution, may be in the same phase (awareness, assessment, renovation, validation, implementation) at the time of review. In instances where a question is not applicable, use N/A.

The FFIEC Year 2000 Examination Procedures, issued in May 1997, are supplemented by this workprogram. (Refer to guidance issued by each respective agency regarding effective dates.) However, examiners may reference and use any part of the original workprogram if additional guidance is sought. Portions of the FFIEC Year 2000 Examination Procedures workprogram may be particularly useful during first time Year 2000 reviews of newly chartered institutions.

OBJECTIVES

1. To determine if the institution is handling Year 2000-related issues in a safe and sound manner and if the project is meeting established timelines and FFIEC key milestone dates.
2. To follow up on results from previous Year 2000 reviews.
3. To determine whether the institution has implemented an effective plan for testing Year 2000 renovated products and implementing these products into its production environment.
4. To assess the adequacy of the institution's Year 2000 contingency plans.
5. To determine whether further corrective action is necessary to assure that Year 2000 readiness is achieved.

PRE-EXAMINATION PLANNING

1. Determine the institution's sources of information systems support for hardware (mainframe, mid-range, networks, personal computers) and related applications, operating system software, and environmental systems. Note whether mission-critical information systems processing is provided internally, externally, or both.
2. Review previous examination, audit, and/or consultant findings relative to Year 2000 issues, particularly results from the institution's last on-site Year 2000 examination/visitation noting significant findings and management responses.
3. Review the FFIEC Year 2000 Workprogram and related workpapers from the institution's last on-site review and any subsequent off-site reviews. Follow-up on any deficiencies noted.
4. Review institution specific information contained in your agency's Year 2000 tracking record/databases, including any information concerning new systems, services, or other changes that have occurred since the previous examination.
5. Review any existing informal or formal regulatory actions as well as resulting correspondence for Year 2000 provisions.
6. For turnkey and serviced institutions, obtain and review a copy of the latest report of examination, Year 2000 visitation report, or shared application software review for the mission-critical service provider or software vendor used by the institution.

SECTION 1 - GENERAL

This section is designed to provide general examination procedures for following up on progress made during the awareness and assessment phases, provide guidance on miscellaneous areas of Year 2000 risk, allow for the evaluation of the involvement and effectiveness of internal/external audit, and provide for an assessment of the institution's indirect Year 2000 risks associated with external sources, customers, and fiduciary activities. For further guidance, examiners should refer to the Interagency Statements on Year 2000 Impact on Customers, Guidance on Year 2000 Customer Awareness Programs and Year 2000 Business Risk.

WORK STEPS

- 1.1 Obtain a copy of the institution's Year 2000 project plan.
- 1.2 Obtain and review board minutes, Year 2000-related committee minutes, if applicable, and copies of management status reports on Year 2000-related activities.
- 1.3 Obtain and review internal/external audit or other qualified sources' plans for, and reports of review of, Year 2000 activities.
- 1.4 Obtain and review the institution's Year 2000 inventory of hardware, software, and environmental systems.
- 1.5 Obtain and review the institution's Year 2000 budget.
- 1.6 Obtain and review any customer awareness pamphlets/letters being distributed by the institution.

EXAMINATION PROCEDURES W/P REF	COMMENTS
GENERAL - AWARENESS	
1.7 Determine if the institution has a reasonable overall Year 2000 strategic plan that, at a minimum, discusses its Year 2000 program management structure, reporting requirements (when and to whom), timeframes and sequencing of Year 2000 efforts, and on an institution-wide basis, what solutions will be used to achieve Year 2000 compliance.	
1.8 Determine if management provides the board of directors, on at least a quarterly basis, status reports detailing the institution's Year 2000 efforts, particularly internal corrective efforts and the ability of the institution's major vendors or servicers to provide Year 2000-ready products and services.	
1.9 Determine if the institution established a committee or other mechanism to ensure Year 2000 efforts are communicated and coordinated among departments institution-wide.	
GENERAL - ASSESSMENT	
1.10 Determine if management has conducted an assessment of all software, hardware, and environmental systems and other computer-controlled systems including:	
a. Prioritizing the inventoried items and identifying those items deemed to be mission-critical.	
b. Describing the method it plans or has used to renovate non-compliant systems.	

SECTION 1 - GENERAL

1.11 Determine if management has a process established to periodically evaluate prioritized inventory to ensure previously assigned priorities remain accurate.

1.12 Assess if the institution has identified and retained enough qualified staff who can assist the institution in becoming Year 2000 compliant.

GENERAL - AUDIT

1.13 Determine the effectiveness of internal/external audit or other qualified sources' involvement in the Year 2000 process by reviewing whether they have:

a. Evaluated the institution's validation and contingency planning processes for service providers, turnkey systems, end-user applications, in-house developed software, and environmental systems, as applicable.

b. Reviewed and assessed controls over the Year 2000 process, particularly emphasizing the validation and contingency planning processes.

c. Determined if those involved in the Year 2000 process have the knowledge and skills to understand and effectively manage Year 2000 efforts.

d. Independently evaluated the Year 2000 project status and the process for reporting to senior management.

e. Assessed the adequacy of business line management and user involvement.

f. Adequately reported their efforts and findings to the board of directors.

GENERAL - MISCELLANEOUS

1.14 Determine if the institution's legal counsel has performed a legal audit that includes a review of insurance policies, public documents, and new and existing contracts or warranties to ensure that they contain appropriate Year 2000 language.

1.15 Determine if management is aware of or contemplates any litigation related to Year 2000. If litigation is anticipated, note the estimated contingency loss and any reserves established for potential losses.

1.16 Assess the reasonableness of the annual budget established for renovation and testing of mission-critical systems (both hardware and software) to make them Year 2000 compliant. Note the amount budgeted for the Year 2000 effort.

1.17 Determine if documentation relating to the institution's Year 2000 compliance efforts has been retained.

1.18 Review the institution's due diligence process for any merger or acquisition plans that may impact the institution's Year 2000 readiness.

SECTION 1 - GENERAL

1.19 Determine if the institution has mission-critical software package(s) or applications that are supported by non-U.S. domiciled companies.

- a. If so, note whether a supervisory authority in the company's home country reviewed, or is scheduled to review, the applications or software packages for Year 2000 compliance. If a review has been conducted, note the results.

1.20 Determine if management has assessed the financial and operational capabilities of its hardware and software vendors to provide Year 2000 processing capabilities.

GENERAL - YEAR 2000 EXTERNAL COUNTERPARTY, CUSTOMER RISK, AND FIDUCIARY ACTIVITIES

1.21 Determine if systems used to conduct trust activities are included in the institution's Year 2000 project.

1.22 Determine if the institution has adequately evaluated and addressed risks associated with:

- a. Holding or managing commercial real estate.
- b. Holding or managing closely held firms.
- c. Fiduciary and transactional counter parties.
- d. Disclosure requirements within the Investment Company Act of 1940 and the Investment Advisors Act of 1940.

1.23 Determine if senior management implemented by June 30, 1998, a due diligence process which identifies, assesses, and establishes controls for Year 2000 risk posed by customers such as funds takers, funds providers, and capital market/asset management counter parties and whether this process includes:

- a. Identifying material customers.
- b. Evaluating their Year 2000 readiness.
- c. Assessing their Year 2000 risk to the institution.
- d. Implementing appropriate controls to manage and mitigate their Year 2000-related risk to the institution.

1.24 Determine if management will have an assessment of individual customers' Year 2000 preparedness and the impact on the institution substantially complete by September 30, 1998.

1.25 Determine if management's review of the adequacy of the loan and lease loss allowance includes Year 2000 customer risk.

1.26 Assess whether the institution has taken measures to mitigate liquidity risk associated with potential customer withdrawal of funds before or after the century rollover. If so, describe.

SECTION 1 - GENERAL

GENERAL - YEAR 2000 CUSTOMER AWARENESS

1.27 Describe what the institution has done to inform its customers of its Year 2000 readiness.

SECTION 2 - RENOVATION

This section is designed to determine whether the institution will complete Year 2000 renovations using methods consistent with safe and sound practices. The renovation phase evaluates Year 2000 code enhancements, hardware and software upgrades, system replacements, and other associated changes. For institutions relying on outside service providers or software vendors, ongoing discussions and monitoring of vendor progress will be necessary.

WORK STEPS

- 2.1 Review the renovation section of the institution's Year 2000 project plan.
- 2.2 Review correspondence to/from the institution's service provider/software vendor.

EXAMINATION PROCEDURES W/P REF	COMMENTS
GENERAL	
2.3 Determine if an adequate process has been established to track renovation efforts of internal mission-critical systems and external systems which interface with mission-critical systems.	
2.4 Determine if the institution has ensured that any replacement products (hardware and software) are Year 2000 compliant or will be Year 2000 compliant within acceptable timelines.	
2.5 Determine if the institution has communicated date format changes with external entities with which it exchanges data.	
LARGE OR COMPLEX ORGANIZATIONS	
2.6 Verify that the institution has implemented change control procedures to ensure all modifications to information systems and their components are properly documented and managed.	
2.7 Determine if the organization has a systems-development life cycle that provides adequate controls over the renovation phase of the Year 2000 process.	
2.8 If vendor technicians and outside consultants are being used, determine if they are subject to the same policies and controls as in-house staff.	

SECTION 3 - VALIDATION

This section is intended to determine the adequacy of the institutions' compliance with guidance and accepted procedures for validating mission-critical hardware, software, and environmental systems for Year 2000 readiness. It is the responsibility of the board of directors and senior management to ensure that Year 2000 risks are effectively evaluated and managed. The most critical phase of the Year 2000 readiness process is validation. For further guidance, refer to the FFIEC Guidance Concerning Year 2000 Readiness.

WORK STEPS

- 3.1 Obtain and review a list of mission-critical systems (e.g., hardware, software, networks, and environmental) noting if systems are developed in-house, or obtained from a turnkey software vendor or service provider.
- 3.2 Obtain and review the Year 2000 validation policies, practices, or procedures.
- 3.3 Obtain and review a copy of the validation strategies and plans for the various information processing environments.
- 3.4 Obtain and review the definition the institution is using for Year 2000 compliance.

EXAMINATION PROCEDURES W/P REF	COMMENTS
GENERAL	
3.5 Determine if the institution has met or will meet the following key milestones in the Year 2000 validation process:	
a. June 30, 1998 - complete the development of their written validation strategies and plans.	
b. September 1, 1998 - commence validation of internal mission-critical systems, including those programmed in-house and those purchased from software vendors.	
c. December 31, 1998 - validation of internal mission-critical systems should be substantially complete. Service providers should be ready to test with customers.	
d. March 31, 1999 - validation by institutions relying on service providers for mission-critical systems should be substantially complete. External testing with material third-parties should have begun.	
e. June 30, 1999 - validation of mission-critical systems should be complete and implementation should be substantially complete.	
3.6 Determine if the written validation strategy and plan for internal and external systems includes:	
a. A description of the testing environment.	
b. Testing methodology (e.g., test scripts, development of test data, proxy testing).	
c. Testing schedules.	
d. The allocation of human and financial resources.	
e. Testing of relevant critical dates.	
f. Documentation of test results.	

SECTION 3 - VALIDATION

g. Testing hardware and software deemed compliant during the assessment phase.

h. Integration testing between the institution's internal systems and interfaces with external entities (foreign and domestic service providers, software vendors or other third-parties) as applicable.

i. Requirements for user participation.

3.7 Assess the adequacy of the institution's Year 2000 testing policies, practices, or procedures including, but not limited to:

a. Reporting the status of Year 2000 efforts to the board of directors on at least a quarterly basis.

b. Routine management reporting (e.g., metrics) to assess the status of testing efforts.

c. Testing mission-critical systems first for business continuity purposes.

d. Maintenance of sound internal controls over the testing process.

e. Requirements for comprehensive testing (baseline, future date, user acceptance, point-to-point, and end-to-end) and system-level reporting to management of significant deviations from the testing methodology as applicable.

3.8 Determine if the institution has:

a. Retained management and staff with appropriate technical knowledge and skills to manage the Year 2000 testing process.

b. Identified staffing and training needs for those involved in Year 2000 testing.

c. Allocated resources (hired, trained, or engaged employees) to perform and analyze tests.

3.9 Review management's process for scoping testing activities and determine whether the process involves or considers:

a. Reviewing the inventory of mission-critical applications and identifying the method used to renovate these applications, such as windowing (including pivot years), date expansion, etc.

b. Compiling a list of the delivery dates for compliant versions of all software developed in-house or obtained from third-parties.

c. Identifying any custom code or features in third-party software.

d. Documenting the network connections and telecommunications dependencies and determining their effect on testing.

e. Documenting the functions, commands, features, transactions, user interfaces, internal/external interfaces, and data files associated with each mission-critical application.

SECTION 3 - VALIDATION

f. Reviewing each mission-critical application to document the application's business or calendar rules.

3.10 Determine the adequacy of the institution's definition of Year 2000 compliance.

3.11 Determine if management's scoping process included testing procedures designed to test all provisions of the organization's Year 2000 compliance definition.

3.12 Verify management reviewed the FRB century date change bulletins and determined testing strategies for programs which interface with a Federal Reserve Bank, if applicable.

3.13 Determine if the testing scope includes testing equipment and hardware with embedded microchips.

3.14 Determine if the institution has taken steps to prevent contamination or corruption of operational systems and related databases during and after the testing process.

3.15 Review the Year 2000 validation process the institution has/will perform for its mission-critical systems and determine if the following types of tests, defined in the Interagency Guidance Concerning Testing for Year 2000 Readiness, are conducted as applicable:

a. Baseline.

b. Future date.

c. User acceptance.

d. Point-to-point.

e. End-to-end.

3.16 Has the institution determined and tested the relevant critical dates necessary to ensure Year 2000 readiness of its mission-critical systems?

3.17 Determine if the institution tests internal and external interfaces.

3.18 Select a sample of test documentation for mission-critical systems and determine if an adequate audit trail exists to support the institution's Year 2000 testing process. Documentation should include:

a. Year 2000 readiness criteria.

b. Types of tests performed (e.g., baseline, user acceptance).

c. Description of the tests noted above.

d. Results of tests.

e. Individuals responsible for acceptance testing.

SECTION 3 - VALIDATION

3.19 Determine whether the institution has or plans to conduct point-to-point testing of mission-critical applications with third-parties with whom it does business, including:

- a. Business partners.
- b. Other institutions.
- c. Payment systems providers.
- d. Clearinghouses.
- e. Customers.
- f. Telecommunications vendors.

3.20 Determine if the institution has or plans to participate in end-to-end testing for transactions of mission-critical systems such as electronic payments.

3.21 Determine whether the evaluation of the testing process included participation by:

- a. Project managers.
- b. System owner/end users.
- c. Independent third-parties (internal/external auditors or other qualified sources).

3.22 Discuss procedures management has in place to ensure test data and test input is retained for testing future releases of the software.

3.23 Evaluate the institution's processes to test that its systems remain Year 2000 compliant following enhancements or modifications. (Clean Management)

SERVICED INSTITUTIONS

3.24 Determine if the institution is coordinating Year 2000 testing with its service providers.

3.25 Evaluate whether the institution has obtained sufficient information to determine if its mission-critical service providers have successfully tested products and services to ensure Year 2000 readiness.

3.26 If the institutions is using proxy testing, determine if management has analyzed the applicability of proxy testing to their institution.

3.27 If proxy testing is used, determine if the institution reviewed and/or provided input to the test scripts used by the user group.

3.28 Evaluate the institution's process for assessing the testing results provided by the party conducting a proxy test.

3.29 Assess the effectiveness of the institution's testing of internal and external interfaces unique to its technology environment and any custom code.

SECTION 3 - VALIDATION

TURNKEY INSTITUTIONS

- 3.30 Determine how the institution is coordinating Year 2000 testing with its software vendor.
- 3.31 Assess whether the institution has determined that mission-critical software vendors have successfully tested their products and services to ensure Year 2000 readiness.
- 3.32 Determine if the institution has joined forces with other institutions using products from the same software vendor, by participating in or relying on user group testing.
- 3.33 If user group testing is used, determine if the institution has evaluated the applicability of the user group test environment to the institution's production environment.
- 3.34 If user group testing is used, determine if the user group test has independence from the software vendor.
- 3.35 If user group testing is used, has management reviewed the scope of the test to ensure the factors in examination procedure 3.9 are adequately addressed. If these factors are not addressed, determine whether management has plans in place to address the remaining risks.
- 3.36 Evaluate the institution's process for assessing the testing results provided by the user group.
- 3.37 Determine if the institution has developed its own independent test plan incorporating results of the software vendor's Year 2000 testing efforts.
- 3.38 Verify that a Year 2000-compliant version of the operating system has been installed in the testing environment.
- 3.39 Review management's plans for using either a date simulation tool or IPL (booting) the system to advance the system clock to future dates. Assess whether these plans allow for an adequate test of the operating system.
- 3.40 Review management's plans or procedures for establishing a future date testing environment. Determine if these plans or procedures address the following issues:
- a. User password expiration.
 - b. Data file and database expiration.
 - c. Software license expiration.
 - d. System authorizations/protections expiration.
 - e. Aging test data files.
 - f. The job scheduling function.
 - g. Archived data.
 - h. Automated housekeeping functions.

SECTION 3 - VALIDATION

i. Internal logging and diagnostic functions.

j. Other devices attached to the system.

3.41 Review management's procedures for returning the system from a post-dated environment.

LARGE OR COMPLEX ORGANIZATIONS

3.42 Describe the organization's process for evaluating and selecting automated testing tools.

3.43 Discuss the organization's program for training employees on validation techniques and the use of testing tools.

3.44 Review the testing plan to determine the methods the organization will use to validate that Year 2000 remediations have not adversely affected the application's structural integrity including:

a. Stress-testing the application to determine if there are any changes to the minimum system configuration requirements.

b. Testing the application's ability to recover from error conditions or system crashes.

3.45 Review the testing plan to determine the methods the organization will use to validate that Year 2000 remediations have not adversely effected the application's functional integrity, and determine if the plan includes:

a. Baseline testing.

b. Unit testing.

c. Integration testing.

d. Regression testing.

e. Point-to-point testing.

f. End-to-end testing.

g. User acceptance testing.

h. Consumer compliance testing.

3.46 Review the testing plan to determine the methods the organization will use to validate that applications will operate in a post-Year 2000 environment.

3.47 Determine if the compliant version of the operating system has been installed in the testing environment.

3.48 Review management's plans for using either a date simulation tool or IPL (booting) the system to advance the system clock to future dates. Assess whether these plans allow for an adequate test of the operating system.

SECTION 3 - VALIDATION

3.49 Review management's plans or procedures for establishing a future date testing environment. Determine whether these plans or procedures address the following issues:

- a. User password expiration.
- b. Data file and database expiration.
- c. Software license expiration.
- d. System authorizations/protections expiration.
- e. Aging test data files.
- f. The job scheduling function.
- g. Archived data.
- h. Automated housekeeping functions.
- i. Internal logging and diagnostic functions.
- j. Other devices attached to the network.

3.50 Review management's procedures for returning the system from a post-dated environment.

3.51 Describe the organization's procedures for selecting contractors, and managing contractors and projects contracted to third-parties.

3.52 Review the organization's procedures for ensuring program changes initiated concurrently with the renovation and testing phases are adequately tested and synchronized into the compliant versions of the programs.

3.53 If the organization acts as a servicer or vendor, determine whether they will (have) share(d) the information generated in the test scoping process with the client institutions.

SECTION 4 - IMPLEMENTATION

During a review of the implementation phase, examiners should focus on the adequacy of management's implementation plan and internal controls governing the migration process. During the implementation phase, systems should be verified as Year 2000 compliant and be accepted by the business users. Any potentially noncompliant mission-critical system should be brought immediately to the attention of executive management for resolution. In addition, this phase must ensure that any new systems or subsequent changes are compliant with Year 2000 requirements.

WORK STEPS

- 4.1 Review the implementation portion of the institution's Year 2000 project management plan.
- 4.2 Obtain and review a copy of the institution's implementation schedule, if it is not included in the project management plan.
- 4.3 Obtain and review updated disaster recovery and contingency plans as well as business resumption plans.
- 4.4 Review correspondence between the service provider or software vendor and its user institutions.
- 4.5 For large or complex organizations, review the integration phase of the organization's system development life cycle.

EXAMINATION PROCEDURES W/P REF	COMMENTS
GENERAL	
4.6 Determine if the institution's plan/process for the implementation of converted or replaced applications and/or system components into the institution's production environment includes:	
a. An assessment of the adequacy of system capacity and DASD/tape storage requirements.	
b. Implementation procedures (steps for getting the program into the production environment and steps for database and archive conversion).	
c. Implementation dates.	
d. Audit review of changes and/or change methodology.	
e. Documented sign-off by management and users.	
f. Methods the organization will use to validate the conversions of existing data files and databases.	
4.7 Determine if management coordinated the institution's implementation schedule with outside entities with which electronic data is exchanged.	
4.8 Determine if the institutions' implementation plan provides for the use of data bridges and filters, where applicable, to allow for the continued exchange of information between compliant systems, non-compliant systems or systems renovated using different date format methods.	
4.9 Determine if adequate controls have been established over the implementation process, and if this process is being applied to Year 2000-related changes.	

SECTION 4 - IMPLEMENTATION

4.10 Determine if system security features have been compromised or removed due to Year 2000 renovations.

4.11 Determine if management has procedures in place to correct program-related faults discovered after implementation and retest those programs after corrections are made.

4.12 Determine if the following items have been updated to reflect any changes resulting from Year 2000 modifications:

a. Balancing procedures.

b. User training programs.

c. Documentation (user manuals, system manuals, etc.).

d. Items maintained in off-site storage (application programs, operating system, documentation, etc.).

4.13 Verify that balancing procedures have been established to address the verification of post-conversion output.

TURNKEY INSTITUTIONS

4.14 Review management's efforts to ensure that all applicable hardware and software at the contracted back-up site has been updated to match Year 2000 compliant versions being used by the institution.

4.15 If the institution has source code in escrow, determine whether the institution received independent verification that the most recent version of the compliant product is being held in escrow.

LARGE OR COMPLEX ORGANIZATIONS

4.16 Review management's efforts to ensure that all applicable hardware and software at the contracted back-up site has been updated to match Year 2000 compliant versions being used by the institution.

4.17 Determine if internal controls governing the change control process are being applied to the Year 2000 project.

4.18 Determine if the organization can recover its production system in the event newly renovated applications fail during the implementation process.

SECTION 5 - CONTINGENCY PLANNING

This section reviews the institution's plans to address remediation and business resumption risks to core business functions that rely on mission-critical systems. Objectives are to determine: 1) that institution management has developed, tested, and implemented contingency plans; 2) whether contingency plans focus on core business functions that pose the greatest risk if lost or seriously compromised by Year 2000 related system failures; and 3) that remediation and business resumption contingency plans contain viable timelines. For further guidance, examiners should reference the Interagency Statement entitled Guidance Concerning Contingency Planning in Connection with Year 2000 Readiness.

WORK STEPS

- 5.1 Obtain and review any reports or documents provided to the board of directors or senior management pertaining to Year 2000 remediation contingency and business resumption contingency planning.
- 5.2 Obtain and review a sample of risk analyses developed for core business functions.
- 5.3 Obtain and review a copy of a report showing the renovation/testing status of all mission-critical systems.
- 5.4 Obtain and review a copy of the institution's Year 2000 remediation contingency and business resumption contingency plans.

EXAMINATION PROCEDURES W/P REF	COMMENTS
GENERAL	
5.5 Determine if the board of directors and senior management have assigned responsibility to appropriate personnel for developing and maintaining a Year 2000 contingency plan.	
5.6 Determine if a process has been established to report progress and changes in the Year 2000 readiness plan to the board of directors and senior management.	
5.7 Determine if contingency planning focuses on identifying, restoring, and continuing core business functions and mission-critical systems that pose the greatest risk to the institution.	
5.8 Determine how Year 2000 contingency planning is coordinated with existing contingency and business resumption plans.	
5.9 Determine if contingency planning for mission-critical systems addresses both remediation contingency planning and business resumption contingency planning.	
5.10 Determine if the organization has identified all customer links into its systems, and addressed such links in the organization's contingency and business resumption planning.	
5.11 Evaluate whether the remediation contingency plan includes:	
a. Possible alternative solutions, including the consideration of alternative software vendors or service providers, in the event remediation efforts are not successful.	
b. Trigger dates for activating an alternative plan, taking into account the time needed to deploy alternative solutions.	
c. Functionality of alternative solutions.	

SECTION 5 - CONTINGENCY PLANNING

5.12 Evaluate whether the **business resumption contingency plan** addresses the following:

- a. Assignment of responsibility to an individual or team for implementing the business resumption plan.
- b. Development of a specific recovery plan for each core business process.
- c. A master list of customers, clients, suppliers, institutions, and government agencies that share data with the institution.
- d. Documentation of products necessary for recovery including machine-readable copies of master and transaction files, printed trial balances, and electronic-text format copies of all master files and trial balance reports.
- e. Printouts of transactions received but not posted as of year-end (e.g., Fed letter, ACH warehouse, ATM).
- f. If environmental systems, hardware, and software at the back-up site are Year 2000 compliant.
- g. If manual processing is to be relied on as a back-up measure, whether the institution has written manual processing procedures to follow and whether they are a viable option.
- h. If key personnel are trained to implement the resumption plan.

3 Evaluate how the institution has verified that its designated back-up site has adequate capacity for its potential Year 2000 demands.

5.14 **Validation of the Business Resumption Contingency Plan**

- a. Determine the adequacy of the method used, or planned to be used, to validate or test the business resumption contingency plan.
- b. Determine that validation or test strategies adequately cover all core business processes.
- c. Identify the party who is responsible for executing the test or validating the plan.
- d. Determine the adequacy of test objectives and scope.
- e. Determine the institution's documentation requirements for business resumption contingency plan testing.
- f. Determine the adequacy of the process for updating the business resumption contingency plan.

SECTION 5 - CONTINGENCY PLANNING

SERVICED/TURNKEY INSTITUTIONS

5.15 Determine if the institution's remediation and business resumption contingency plans are consistent with those of its third-party software vendor or service provider.

LARGE OR COMPLEX ORGANIZATIONS

5.16 Determine if the description of core business processes distinguishes between the servicer's internal processes and the mission-critical functions of its client institutions.

5.17 Identify how the organization has assigned roles and responsibilities for maintaining client contacts during the business resumption process.

5.18 Describe the organization's efforts to communicate its Year 2000 remediation contingency and business resumption contingency plans to its client institutions.

5.19 Identify how the organization arrived at an understanding with its client institutions as to the minimum service levels to be maintained in a contingency environment.

5.20 Determine if the organization's contingency plan addresses the restoration of these minimum service levels.

5.21 Describe the steps taken by the organization to ensure continued service for client institutions if telecommunications or power problems are experienced.

5.22 Describe the provisions that have been made for testing contingency plans and processes relating to Year 2000 and the services provided to client institutions.

5.23 Determine if the organization has clearly identified the type of business resumption plan testing to be used for each core business process.

5.24 Evaluate whether adequate provisions have been made to provide a copy of master files and trial balances as of year-end 1999 in an electronic format to all serviced client institutions.

SECTION 6 - EXAMINATION CONCLUSIONS

Questions in the Examination Conclusions section are designed to narrow the examiners focus to the primary risk areas associated with the final phases of the Year 2000 project as well as concerns in the areas of Year 2000 indirect risk. Responses should be well documented within the workpapers which accompany this Workprogram. Items detailed below should be addressed within comments prepared for the Report of Examination or Visitation Memorandum resulting from the current on-site review.

	COMMENTS
<p>Develop summary comments for the open section of the report of examination/visitation memorandum. Comments should address the following topics:</p>	
<p>6.1 Assign an overall Year 2000 rating to the institution/organization based on the findings of the review.</p>	
<p>6.2 Describe whether the institution has a formal Year 2000 project plan, if the plan is reasonable, and if the institution is following the plan.</p>	
<p>6.3 Note whether the institution's Year 2000 project plan establishes reasonable and attainable deadlines that will enable the institution to meet the key milestone dates set forth in the Interagency Statement on Guidance Concerning Testing for Year 2000 Readiness.</p>	
<p>6.4 Provide a brief description of the institution's reporting structure, including frequency, in relaying Year 2000 compliance efforts to the board of directors.</p>	
<p>6.5 Address the institution's efforts to monitor the progress of its service providers and software vendors in becoming Year 2000 compliant.</p>	
<p>6.6 Discuss whether data-processing service provider(s) or software vendor(s) have plans to deliver a remediated product which will allow the institution to test within the key milestone dates set forth in the Interagency Statement on Guidance Concerning Testing for Year 2000 Readiness.</p>	
<p>6.7 Provide a brief description and assessment of the institution's testing methodology.</p>	
<p>6.8 Provide an assessment regarding the adequacy of the institution's test plan.</p>	
<p>6.9 Describe if the institution has adequate remediation and business resumption contingency plans.</p>	
<p>6.10 Briefly describe management's plan to address indirect Year 2000 risks such as those associated with counter parties, customers, and fiduciary activities.</p>	
<p>6.11 Describe efforts implemented by the institution towards making customers aware of its Year 2000 efforts.</p>	
<p>6.12 Discuss any major problems which are anticipated by management, towards achieving Year 2000 compliance.</p>	

SECTION 6 - EXAMINATION CONCLUSIONS

6.13 List the name(s) of individuals responsible for the institution's Year 2000 efforts, particularly the designated Year 2000 project manager, and describe their status in the organizational structure.

6.14 Detail any exceptions or weaknesses noted with the institution's Year 2000 compliance program. Provide management's response detailing commitments for corrective action.

6.15 Detail efforts made by management to correct deficiencies noted at prior reviews or note previous deficiencies which still remain unresolved.

6.16 State whether the institution has managed its Year 2000 business risk and contingency planning efforts in a safe and sound manner.

6.17 List the names and titles of management members with whom Year 2000 findings were discussed.

6.18 State whether Year 2000 examination results were discussed with the board of directors, if applicable, or a designated committee thereof.

The following areas should be discussed in the confidential section of the report of examination or visitation memorandum as appropriate:

6.19 Detail recommendations for follow-up action or recommendations for enforcement action. If enforcement action is recommended, contact the appropriate management official for your regulatory agency.

6.20 For bank and non-bank service providers and software vendors, prepare a list of serviced institutions which are currently under contract with that provider. Include name, city, state, and charter type.

6.21 List serviced or turnkey institutions which according to the servicer or vendor will need to take specific action, such as a conversion or upgrade, to achieve Year 2000 compliance.


TESTIMONY FOR SENATE BILL NO. 2303

Senate Industry, Business and Labor Committee



Testimony of Shawn Cleveland Goll, Y2K Project Manager, BNC National Bank

BNC National Bank board and senior management have been actively engaged in managing the Year 2000 Project since June of 1997. Bank management has consistently allocated both human and fiscal resources consistent with what it believes are the bank's requirement to comply with the Federal Financial Institution Examination Council (FFIEC) guidelines. On more than one occasion, management has made the decision to defer investments in alternate technologies to ensure those processes and systems currently in place achieve Year 2000 readiness according to the FFIEC guidelines. To date, BNC has taken the following measures:

- Established a Year 2000 Project Team in June 1997 (currently includes 15 employees);
- Assessed all software, hardware, environmental and other computer-controlled systems; prioritized and identified those deemed mission-critical;
- Established a Year 2000 budget of \$273,000 (currently have spent \$58,000 with \$80,000 more to be booked by the end of the first quarter 1999);
- Updated and/or replaced all identified non-compliant hardware and software;
- Tested all identified mission-critical systems;
- Identified and assessed the Year 2000 risk posed by customers;
- Established measures to mitigate liquidity risk associated with potential customer withdrawal of funds before January 1, 2000;
- Communicated the bank's Year 2000 readiness to customers via letters, brochures and seminars;



Established a Year 2000 Contingency Plan which includes:

- backup Hot Sites
 - generators
 - software conversion
 - year-end cut-off on December 30, 1999
 - no vacation policy for months of November and December 1999 and January 2000
 - extended hours
 - manual processing
- 
- 

Statement and Testimony
Joel Gilbertson, Executive Vice President & General Counsel
Independent Community Banks of North Dakota
In Support of S.B. 2303

Mr. Chairman, members of the Committee, I am Joel Gilbertson, Executive Vice President and General Counsel of the Independent Community Banks of North Dakota, with offices in Bismarck. ICBND is a statewide association of 95 independent community banks located throughout the state. Our member banks are located in communities of all sizes, and one of our association's primary objectives is to preserve the tradition and the benefits of community banking.

I am pleased to appear on behalf of our association in support of S.B. 2303.

Banks were among the first institutions to embrace the use of computers both to record accounts and to make transactions. Today, by one estimate, 90 percent of all bank assets are electronic entries in data bases and virtually all bank transactions involve electronic processing.

Because of the obvious dependence on computers and the obvious sensitivity to problems with the millennium bug, and perhaps as well because of extensive regulatory activity, I think it is fair to say that the banking industry has done as much or more than any other industry in preparing for the Year 2000. In fact, at least two independent studies, by the Garner Group and Cap Gemini, have concluded that the banking industry is ahead of all others in Y2K preparedness. In addressing this issue, John Koskinen, chair of the President's Council on Year 2000 Conversion has said that banks are the most heavily regulated industry in the country and get ratings of 97% to 98% compliance in every survey he has seen.

The Year 2000 problem is pervasive and complex. However, the various bank regulators have been very active in assuring that banks are ready.

The Federal Deposit Insurance Corporation (FDIC) is the regulator that is responsible for insuring deposits and a regulator responsible for supervising state-chartered banks that are not members of the Federal Reserve System. The FDIC has identified Year 2000 readiness oversight as its highest safety and soundness priority.

It is very important to note that the Year 2000 date does not affect any customer's deposit insurance coverage. No matter what difficulties, if any, financial institutions may encounter, each depositor will remain fully insured up to the statutory limit of \$100,000.

A national group of federal regulators has dealt in great detail with Year 2000 readiness as well. The Federal Financial Institutions Examination Council (FFIEC) is composed of representatives from the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, and the National Credit Union Administration.

The FFIEC has established a number of deadlines to be followed by the various banks they supervise. The FFIEC deadlines are as follows:

- ◆ **June 30, 1998** - Institutions should complete the development of their written testing strategies and plans.
- ◆ **September 1, 1998** - Institutions processing in-house and service providers should have commenced testing of internal mission-critical systems, including those programmed in-house and those purchased from software vendors.
- ◆ **December 31, 1998** - Service providers should be ready to test with customers.

- ◆ **March 31, 1999** - Testing by institutions relying on service providers for mission-critical systems should be substantially complete. External testing with material other third parties (customers, other financial institutions, business partners, payment system providers, etc.) should have begun.
- ◆ **June 30, 1999** - Testing of mission-critical systems should be complete and implementation should be substantially complete.

To date, the FFIEC regulators appear to be in step with their proposed deadlines.

I hope the foregoing has assisted in giving you information and background about the banking industry's plans and efforts to get ready for the Year 2000. Y2K is a very serious and real problem for our industry. However, it has not been taken lightly. Millions, perhaps more likely billions, of dollars have been or will be spent to assure as smooth a transition as is possible. Aberrations will occur, but we are hopeful the popping of champagne corks at midnight on January 1, 2000 will bring with it as few problems as possible for bank customers in North Dakota and around the country.

In the event that, because of reasons beyond the control of banks, problems occur, S.B. 2303 will allow actual economic damages but place lid on a huge windfall against banks when they fulfilled the Year 2000 requirements of their regulators in an environment that is the most regulated of any. It some protection but not unlimited protection. It also inserts other protections so that it is clear the fault of all actors who play a role in a loss or damage will only be responsible for their percentage of that fault.

Our community bankers are hopeful you appreciate the work that has been done to prepare for the Year 2000. Our community bankers also have tried to be sensitive to the needs

and claims of others in an attempt to balance those needs with the real world efforts of our industry to prepare for the new millennium.

We urge your vote for a Do Pass recommendation on S.B. 2303. Thank you.

N.D. banks tackle Y2K issue

JOE GARDYASZ, *Bismarck Tribune*

Planning and precautions being taken by North Dakota's banks should protect consumers from problems resulting from possible Year 2000 computer glitches, banking officials say.

More importantly, people should be aware of possible scams by those who may want to convince them to withdraw their money from the bank for "safekeeping," says a state official.

Banks and thrifts throughout the state have already spent money and time preparing for possible problems, says Roger Monson, a Finley banker and president of the North Dakota Bankers Association.

"They have tested their systems, they have written contingency plans and they have been and will continue to be examined on their Year 2000 efforts," Monson said.

Ahead of the task

June 30 is the deadline given by the Federal Deposit Insurance Corp. for all banks to have tested and validated all mission-critical systems, including an independent review of their results. The agency does not disclose compliance figures for individual states, but estimates that nationally less than one-half of 1 percent need to improve their compliance efforts.

"We feel very good about where we're at, and that's because for over two years the banks have been going through these plans that are being looked at by examiners," said Jim Schlosser, NDBA's executive director.

"Nobody can say with certainty that there won't be any glitches, but if there are, there are these contingency plans in place to take care of any problems that do arise."

Financial institutions are the only industry that has Year 2000 federal regulatory requirements. That, and the fact that all deposits will continue to be insured up to \$100,000 by the FDIC, means banks remain the safest place to keep your money, Monson says.

Also known as "the Y2K Bug" or "the Millennium Bug," the turning of the calendar on Jan. 1, 2000, could potentially cause computer systems to fail if the programs written to recognize two digits for the year think 00 represents 1900, not 2000.

Making sure their lights stay on and that tellers know how to process payments manually are just some of the procedures banks are working out.

Contingency plans

At BNC National Bank in Bismarck, the bank's contingency plan includes wiring the building to install a backup electrical generator to power their computer system in case the power fails.

From testing their computer system, they've reached a comfort level that it will work Jan. 1, said Shawn Cleveland Goll, the bank's Y2K compliance officer.

"What we can't test are systems outside our control, such as utilities," she said. "We have no idea what the likelihood is that there will be power or not. But because we can't test for it, that's why we feel it's prudent to include it in our contingency plan."

Other contingency steps being taken by banks include plans for longer hours to handle increased customer volume, no-vacation policies to ensure staff will be available late in the year and training on manual procedures.

Kirkwood Bank & Trust officials have made arrangements for another institution on another power system to handle their processing, if necessary. As another alternative, they also have a backup generator lined up to lease, said Dave Kusler, the bank's cashier.

Another contingency that they're planning for is possible longer hours needed in the event of a telecommunications failure, which would take out both phones and automated teller machines.

The bank is also testing its computer system.

"We don't at this time foresee any problems," Kusler said.

The U.S. Treasury plans to print an extra \$50 billion in anticipation of the public's increased desire for cash that weekend, NDBA's Schlosser said.

For safety reasons, people shouldn't take out more than they otherwise would for a holiday weekend, he added.

Attorney general's warning

Keeping deposits in the bank is the safest route, North Dakota Attorney General Heidi Heitkamp says.

"Customers need to understand that this is not Armageddon," she said. "There will be plenty of doom-sayers ready to proclaim 'The world is coming to an



By MIKE McCLEARY of the Tribune

Kirkwood Bank and Trust teller Dee Stuhlmueller uses her computer to help customer Sharon Weber.

Steps customers can take to protect themselves

Here are steps bank customers can take to protect themselves. According to Attorney General Heidi Heitkamp, these suggestions are generally wise steps to take at any time.

- Keep good records of all your banking transactions, especially for the last six months of 1999 and until you get several bank statements in 2000. These records should include documentation of your deposits, investments, ATM withdrawals, and loan payments (credit cards, mortgage, auto loan, etc.). Bank statements and transaction receipts also are among the documents you should be saving. These records will help your bank and you quickly resolve any errors that may occur.

- Check your transaction receipts against your periodic statements. If there's a discrepancy, contact your institution immediately.

- Stay informed. Pay special attention to the mailings from your bank and other institutions. These often include helpful tips. If you have questions or concerns, speak with an employee of your bank who is knowledgeable about the institution's Year 2000 program.

end' for various motives. Yes, Y2K is a computer problem, but the customers' money won't disappear and be lost," she said. "The U.S. government is not going to stop working and deposits will still be insured by the FDIC."

Heitkamp also warned residents to be concerned about scam artists who offer to "hold" your money through the date change.

"Scam artists will try to take advantage of consumers' fears by developing scams that lure unsuspecting individuals into making bad decisions about their money.

"Scam artists may try to persuade consumers that Year 2000 computer problems will create havoc on our economy. They may describe frightening scenarios of

banks shutting down," said Heitkamp.

She encouraged consumers to watch out for scam artists who try to:

- Convince consumers that the dire predictions regarding loss of financial security due to Year 2000 problems are true.

- Persuade consumers to invest in "special" or "secret" products, companies, or accounts that will generate tremendous profits.

- Advise individuals to withdraw their money out of banks, credit unions, or other financial institutions and turn it over to them for "safekeeping."

"Your money is safest in the bank. Educate yourself about the Year 2000 situation and what banks are doing to protect consumers," she said.

SB 2303
HOUSE Industry, Business & Labor Committee
Comments by Jim Schlosser, Executive Vice President
North Dakota Bankers Association

Year 2000 Glitches

We can trace the Y2K problem back to "tabulating equipment" that businesses and government agencies relied on before computers became common in the 1960's and 70's. The tabulating machines read, sorted and tallied information entered on millions of envelope-size cards. Each card held only a small amount of information so abbreviations and codes were used for words and numbers. For example, typists recorded the year 1955 onto a card by punching holes for "55". The same shorthand method continued in the computer age because of costs and storage problems with early computers before the invention of computer chips. The two-digit arrangement for calendar years worked fine until now. On Jan. 1, 2000, if the date is simply recorded in a computer as 00, the computer assumes it means 1900, not 2000, unless the computers and computer chips are reprogrammed.

What financial institutions have been doing to prepare for Year 2000.

North Dakota banks, thrifts and credit unions, whether large or small, have been preparing and testing for the year 2000 for over two years. **Federally-insured financial institutions are the only businesses that have year 2000 state and federal regulatory requirements** (see attached articles). Federally-insured financial institutions in the state have tested their systems, written contingency plans, have been and will continue to be examined through 1999 (quarterly Y2K examinations are scheduled). **It is estimated that \$8 billion has been spent to date by financial institutions in the United States to prepare for Y2K and banks are rated number one in Y2K preparedness by leading computer industry experts.**

North Dakota's Attorney General called a press conference on Jan. 21 to urge North Dakota residents to "keep their money in the bank". A theme has been adopted in a joint effort with the North Dakota Bankers Association "There is nothing safer than money in the bank" (see attached flyer). The Attorney General is quoted as saying "your money is safest in the bank" and the Commissioner of Banking recently stated before a House appropriations subcommittee, **"North Dakota financial institutions should be fully prepared for the century date change and I expect very little disruption, if any, to customers."**

North Dakota financial institutions are required by federal regulators to have **special contingency plans** in preparation for the year 2000. Banks and thrifts have contingency plans at the present time, which worked very well during the extensive flooding in the Red River Valley in 1997. Banks and thrifts that lost buildings due to the flooding and fire on Saturday were handling transactions and processing checks on the Monday following the disaster.

Legislation dealing with state and political subdivisions.

The interim Information Technology Committee and the Legislative Council introduced House Bill 1037, which gives the state and political subdivisions immunity for any claims arising out of the failure of computer hardware or software if the state or political subdivision has made a "good-faith effort" to make the hardware, software and computers comply with the year 2000 date change.

While attending the hearing on this bill, I was encouraged by the position of the trial lawyers on this issue. While a representative of the Trial Lawyers Association stated there should not be complete immunity by the state and its political subdivisions, he did agree that legislation is necessary to limit damages resulting from outside businesses and agencies causing damages because they are not Y2K compliant. SB 2303 does fit within the guidelines established by the trial lawyers in their testimony before the House Government and Veterans Affairs Committee on HB 1037.

Why is this bill necessary?

Financial institutions in this state have invested an unprecedented amount of resources to achieve year 2000 readiness, and are doing so under the strictest scrutiny of federal and state regulators, congressional oversight, financial markets, the press and millions of customers. The goal of the enormous effort is a smooth transition into the next century for all banking services.

As financial institutions proceed to finalize the Y2K preparation, it is increasingly clear that they may face another expenditure that is even larger than the \$8 billion being spent by the industry on Y2K readiness — and that would be the cost of litigation brought by individuals or class action plaintiffs not customers of federally-insured financial institutions seeking damages for alleged Y2K disruptions. While financial institutions are confident that they would be successful in defending these actions, **the cost of defending frivolous lawsuits would be passed on to their customers.**

Financial institutions are not seeking a limitation of liability because they are not prepared. In fact, most financial institutions are well ahead of the government-mandated deadline of testing of all systems by June 30, 1999. There is inter-dependency between the systems used by financial institutions and external interfaces. Federally-insured financial institutions have no control over transportation delays, energy failures or communication problems.

Financial institutions in the state are not seeking to avoid liability. **The bill contains no caps on actual damages suffered by parties who have a privity of contract with a federally-insured financial institution.** Financial institutions and credit unions are only seeking to eliminate abusive and frivolous suits and claims for punitive damages and to clarify liability for actual damages directly caused by Y2K disruptions. Application of this bill is conditioned on a federally-insured financial institution demonstrating good-faith implementation of a Y2K conversion plan.

Finally, one of the major purposes of the bill is to protect the safety and soundness of federally-insured financial institutions by eliminating excessive or punitive damages. The specific provisions of the bill will be reviewed by the general counsel for NDBA, Marilyn Foss, and I ask your strong consideration for this legislation, which is of major importance to nearly 200 financial institutions in the state with approximately 400 facilities and 8,000 employees.

TESTIMONY FOR SENATE BILL NO. 2303

House Industry, Business and Labor Committee

Testimony of Shawn Cleveland Goll, Y2K Project Manager, BNC National Bank

BNC National Bank board and senior management have been actively engaged in managing the Year 2000 Project since June of 1997. Bank management has consistently allocated both human and fiscal resources consistent with what it believes are the bank's requirement to comply with the Federal Financial Institution Examination Council (FFIEC) guidelines. On more than one occasion, management has made the decision to defer investments in alternate technologies to ensure those processes and systems currently in place achieve Year 2000 readiness according to the FFIEC guidelines. To date, BNC has taken the following measures:

- Established a Year 2000 Project Team in June 1997 (currently includes 15 employees);
- Assessed all software, hardware, environmental and other computer-controlled systems; prioritized and identified those deemed mission-critical;
- Established a Year 2000 budget of \$273,000 (currently have spent \$58,000 with \$80,000 more to be booked by the end of the first quarter 1999);
- Updated and/or replaced all identified non-compliant hardware and software;
- Tested all identified mission-critical systems;
- Identified and assessed the Year 2000 risk posed by customers;
- Established measures to mitigate liquidity risk associated with potential customer withdrawal of funds before January 1, 2000;
- Communicated the bank's Year 2000 readiness to customers via letters, brochures and seminars;

Established a Year 2000 Contingency Plan which includes:

- backup Hot Sites
- generators
- software conversion
- year-end cut-off on December 30, 1999
- no vacation policy for months of November and December 1999 and January 2000
- extended hours
- manual processing