Frontier
Telephone Group

frontier

180 South Clinton Avenue
Rochester, NY 14646

Kay Flynn
Florida Public Service Commission
Division of Records and Reporting
2540 Shumard Oak Blvd.
Tallahassee, FL 32399-0850

March 16, 1999

Dear Ms. Flynn;

Attached is Frontier Communications' response to the Year 2000 request for information of March 5, 1999. This response is made on behalf of:
Frontier Communications Services
Frontier Communications International
Budget Call Long Distance
Frontier Telemanagement
Frontier Communications of the West
Frontier Communications of the South

This information package should address all the concerns included in the data request. If you have any further questions, please contact Jerry Bonello at (800) 283-6903.

Sincerely,

Christine Burke

Christine Burke
Senior Analyst, Regulatory
Frontier Telephone Group

Florida Public Service Commission
Division of Records and Reporting
2540 Shumard Oak Blvd.
Tallahassee, FL 32399-0850

March 16, 1999

Re: YEAR 2000 READINESS DISCLOSURE

Thank you for your interest and concern regarding Frontier's preparations for the transition into the Year 2000. We receive many similar questions about the steps Frontier is taking to be ready for this critical date. In order to respond to the numerous inquiries, we have put together the following information regarding our Year 2000 Project:

Awareness - Communication of the impact of the calendar change is being shared throughout our organization. Executives, managers, and other employees have been notified that the situation may impact not only the major applications that they use, but also their desktop applications, including personal software and hardware, and core business systems.

Inventory & Assessment - Frontier is documenting all software, hardware, and data interfaces that it can identify as possibly being impacted. This process was initiated in 1996. Mission critical applications have been assessed to determine the extent of their vulnerability. Other, less critical systems have also been assessed or are scheduled for assessment in the near future. The assessments are being used to budget the remediation project, identify needed development and testing tools, and recruit and retain the necessary resources to work on the project.

Software Remediation & Testing - Many internal projects involving the correction of potential date problems are well underway. Our methodology is to seek each date reference, modify the manipulation of that date as necessary, and test the modifications for effectiveness when processing current dates, dates that cross over from 1999-2000, and special dates after the year 2000, such as 02/29/2000. Frontier's internal information technology systems were 85% year 2000 ready by 12/31/1998, with the balance of the systems anticipated to be year 2000 ready by 03/31/1999. System testing will continue throughout 1999 and into 2000 to the extent Frontier deems such testing to be necessary. In addition, Frontier's Year 2000 assessment and remediation strategy has been nationally recognized with a nomination for a *Computerworld Smithsonian* award in the Business & Related Services category.

External Communication - Frontier, like all businesses should, is continuing to contact its software, hardware and business suppliers to determine their plans for full year 2000 compliance.

Network & Facilities - Frontier has developed, and continues to develop, detailed plans to evaluate devices which comprise our communications network. Frontier anticipates its internal network facilities to be year 2000 ready by 6/30/1999. The need for testing appropriate network element equipment and software is being determined and coordinated with Frontier suppliers and business partners, and discussions between carriers are underway related to inter-carrier testing. As carrier to carrier interoperability testing is just being implemented in the telecommunications industry, Frontier, like other carriers, is unable at this time to accurately assess the year 2000 readiness of its network when connected to the public switched network or other carrier networks. In order to minimize potential risks, Frontier plans to participate in Carrier interoperability testing throughout 1999. Similar plans are also in development for our building facilities, which include security systems, safety equipment, and other date-embedded devices.

Centrex and Voice Mail – The software for Frontier's switching equipment that supports its Centrex and voice mail services is currently being upgraded to the manufacturer's newest versions. During these software upgrades, Year 2000 testing is performed, or in some cases the testing is being performed at the manufacturer's lab facility. Once the upgrades are completed the switching equipment should be Year 2000 Ready.

Your concerns regarding the millennium date problem are understandable. Frontier is treating the Year 2000 issue very seriously. Our goal is to minimize the potential for disruption to customer service or product delivery. We are diligently taking steps to implement a smooth transition and to ensure the continued availability of premier integrated telecommunications products and services through and after January 1, 2000. As you know, no one can predict with certainty what systems or facilities may ultimately be affected by the complex inter-relationships that exist among many businesses up and down the supply chain and between their operating systems and applications; therefore this letter is not a warranty or certification of Frontier's Year 2000 readiness and should not be relied upon as such.

I hope this information is sufficient to address your inquiry. If not, or if you require any additional information, please feel free to contact us at (800) 283-6903, or e-mail our project team at year2k@frontiercorp.com.

Sincerely,

Gerald J. Bonello
Director, Year 2000 Development
Frontier Information Technologies

YEAR 2000 READINESS DISCLOSURE

Year 2000 Questions

Please provide your year 2000 contact information.

Company: Frontier Communications
Address: 180 S. Clinton Ave.
Rochester, NY 14646
Phone: 800-283-6903
Fax: 800-283-6903
Contact: Jerry Bonello
E-Mail year2k@frontiercorp.com

1) What is Frontier's definition of "Year 2000 Compliance?"

When we say "Year 2000 Compliant" in our Year 2000 informational material we mean, specifically:

- No valid value for date related data will cause an error or failure in any desired operation (IO, modification, reference, comparison, display, etc.) within that system.
- Manipulations and comparisons of date related data will produce the desired results for all valid dates within the scope of the application.
- Where feasible, significant external customer reporting will be modified to display the year in CCYY format.
- The year 2000 will be recognized as a leap year.

From time to time we expect to include additional criteria that is determined to be necessary for successful implementation of our Year 2000 program.

2) Does your company use computerized systems that may be impacted by the year 2000 problem? Have you performed an assessment of these systems? What are the results of these assessments? Have you experienced year 2000 failures to date?

Frontier is affected much as other businesses are with respect to facilities, hardware and software that are used across the economy. As a telecommunications and information firm, Frontier's business operations may be affected in three major categories:

- Internal computer systems and PCs (desktops and laptops)
- Vendor supplied hardware and software
- Telecommunications network operations and support, including interconnection and interoperability with other carriers, and building/facility equipment.

Mission critical applications have been assessed to determine the extent of their vulnerability. Other less critical systems have be also been assessed or are scheduled for assessment in the near future. Applications that process dates two to three years in advance have already had to be addressed. This would include calculating the end date of a contract when given a start date and duration. As 1999 progresses, other such milestones will be approached, verifying the thoroughness of our remediation project. It is important to recognize that early failures would appear in the support systems not in network elements and therefore would not be customer impacting.

3) Does your Company have a Year 2000 plan or strategy in place? Is it written?

Our assessment phase prompted the initialization of several projects (conversion and replacement) across multiple platforms to address the millennium problem. Separate project plans have been created at the platform level and are managed by regional project managers. Each project manager provides regular status updates to a central program manager who then reports the progress to Frontier's Y2K Executive Steering Committee.

4) If you are not fully compliant today, state where you are in each phase and when you plan to complete each phase.

As of 4th Quarter 1998	Inventory & Assessment	Remediation	Testing	Implementation	Verification & Certification	Targeted Completion
Network Elements	95%	50%	40%	40%	40%	6/30/99
Support Systems	100%	90%	60%	60%	60%	3/31/99
Administrative Systems	100%	80%	60%	60%	60%	3/31/99
Infrastructure	95%	50%	40%	40%	40%	6/30/99
Facilities Systems	75%	20%	10%	10%	10%	9/30/99

Definitions:

Network Elements – systems, components, embedded devices or software that directly affect customers' transmission and/or reception of telecommunication services.
Support Systems –operations support and customer support systems.
Administrative Systems - payroll, human resources, finance and other administrative systems.
Infrastructure – LAN servers and other equipment, desktop PCs, mainframe, operating systems, system software, embedded devices.
Facilities Systems – HVAC, FAX, security and alarm systems, embedded devices and other similar systems.
Inventory and Assessment – activity to identify potentially affected items, systems, software and equipment, to ascertain compliance status.
Remediation – activity to repair, replace or retire affected systems.
Testing/Verification – activity to test, verify and implement corrected systems.

Frontier's year 2000 project began in 1996. Since that date, our methodology has been to employ a fixed window, procedural code solution to allow us to quickly code, test and implement remediated code back into production, lessening the impact on our day-to-day business. Standard year 2000 compliant date routines were developed and are being utilized as well as various testing tools. We are reasonably confident that all of our system impacts have been identified; however, we are continuing to perform assessments (as necessary) and identify solutions for impacted network elements which cannot be corrected in the same way our internally developed software systems can be.

5) Are you using third party vendors or internal resources to solve your year 2000 problem? Identify your vendors. What warranties are your year 2000 vendors providing?

Frontier is utilizing the services of multiple vendors and consultants to perform year 2000 remediation and to augment our own staff on remediation projects. Some of these include Platinum Technologies, Keane Inc., Computer Aid and others. However, no one can predict with certainty what systems or facilities may ultimately be affected by the complex interrelationships that exist among many businesses up and down the supply chain and between their operating systems and applications; therefore most vendors are not providing a warranty or certification of Year 2000 readiness.

6) How many resources do you have assigned to your year 2000 project? What is the magnitude of your compliance effort? How many programs and lines of code are impacted?

Frontier has approximately 30-40 FTE (Full time equivalent) resources assigned to various phases of the project. We estimate resources will be assigned at this level until and possibly after the change to year 2000. In total, our internal systems constitute 21 million lines of code in 12,000 programs.

7) Does your company exchange electronic data with vendors, suppliers and customers? What are the compliance plans for these data feeds? How will you prevent non-compliant data in these data feeds from corrupting your compliant databases? What contingency plans do you have to prevent this?

Frontier processes many electronic data interfaces both entering and leaving our systems. Many of these are industry standard formats, while others are mutually agreed upon formats between our business partners. We use a fixed window of 70 to interpret any date data in these feeds that do not contain a 4-digit year. This indicates that years 70-99 will be interpreted as 1970-1999 and 00-69 will be 2000-2069. Data will be validated against these rules and rejected to prevent non-compliant data from entering our systems just as the data today is edited to be sure it falls within pre-defined business rules. If our testing uncovers any issue with this process, Frontier will investigate developing contingency plans to prevent non-compliant data from being processed.

8) Does your Year 2000 plan include verifying the compliance of your vendors and suppliers on which you are dependent? Does it take in to account the failure of major customers and the possible loss of business associated with their ability to become compliant?

Just as you have concerns and are contacting your vendors, Frontier is contacting its software, hardware and business suppliers to determine their plans for full year 2000 compliance. We are continuing to contact our vendors to determine their product release schedules so that we may integrate and test them with our internally developed systems well in advance of Year 2000. Frontier is also working closely with our major customers to assist in their Year 2000 effort where ever possible. Timely communication of compliance issues and open sharing of information are the best ways to minimize impacts to both of our businesses as a result of the Year 2000.

9) Year 2000 problems can cause problems in embedded systems such as heating, cooling, security systems and elevators. How does your year 2000 plan address these issues?

Frontier has many locations that need to be addressed. Many of Frontier's properties are leased and as such we are heavily reliant on the owners of the buildings to check for Year 2000 impacts. Frontier is continuing to work closely with the manufacturers of these systems to be sure Year 2000 issues are being addressed. Additionally, where feasible, Frontier is testing these systems by resetting the dates and allowing the device to roll over from 1999 to 2000.

10) What is Frontier's Network and IT conversion strategy?

Frontier is focused on a methodical and thorough review of our internally developed software and systems, the testing of vendor software products, and implementation of a deliberate process to correct, work around or replace code, or other items that would not be Year 2000 compliant. Techniques include the following:

- Relying on procedural code changes to achieve compliance. This means using a fixed window of 70 to interpret the century (i.e. years 00-69 are 2000-2069; 70-99 are 1970-1999). This arrangement affords greater confidence of correct modifications and maintains a relatively consistent format for users.
- Testing modifications by warping the **system date** and data in order to assure that the system functions properly with these date values. This is done using the current date, dates that cross over from 1999 to 2000, and various other year 2000 dates. Some of these dates include: 12/31/1999, 1/1/2000, 2/29/2000, 12/31/2001 and 12/31/2005. Other dates are tested if they are deemed appropriate to test hardware/software functionality.
- Simulating separate year 2000 environments for its network and information technology systems to test systems hardware and software and interoperability among carriers for compliance. However, please keep in mind that given the enormous array of connections and ties among unaffiliated entities that comprise the nation's telecommunication network no one can simulate a complete Year 2000 environment.

11) What Contingency plans have you developed? Do these plans address failure to meet current remediation or system replacement schedules? Do they address business processes that fail despite these remediation efforts? When would you determine that it is necessary to implement these plans?

Frontier has developed a contingency matrix of potential problem areas along with their respective probabilities of failure and severity level. However, we feel contingency plans will only be necessary for critical systems where remediation or replacement projects are not on schedule. Frontier does not currently see a risk associated with the schedule for completing the existing year 2000 projects. Year 2000, however, is the corporation's top priority. As the time-frame draws near, or planned system replacement schedules are determined to be at risk, additional resources will be transferred to the project to assure successful completion.

Each remediation or replacement project has critical milestones that are closely tracked. If for example, a project to replace a system has not reached these milestones that were determined by upper management, the contingency to remediate the existing system would kick in and resources would be re-assigned to the remediation project. These milestones are dependent on the remediation estimate determined during the assessment phase and vary according to the year 2000 impact on the system.

Frontier has existing staff assigned to be on-call for both IT system failures and network outages. This coverage is 24x7 to assure quickest possible response. Should any outages occur, production problems such as this become the highest priority and any additional resources necessary will be diverted to solve the problem. Frontier is currently investigating several changes to this policy such as requiring these on-call personnel to be on-site, adding additional resources and limiting vacation to be sure that all of the proper resources will be available to quickly address any issues.

12) What test plans and test results will Frontier provide their customers? How can I test my services with Frontier?

Frontier is dedicating considerable resources in investigating and solving any year 2000 problems it may encounter with its network and systems. Currently, Frontier's remediation and testing results are maintained within a proprietary format that is not easily understandable outside the context of our internal systems and processes. Therefore we have made a strategic decision to focus all of our efforts on the remediation and testing process and not divert our resources by providing testing plans and results in a user-readable format. By maximizing our remediation and testing resources we can focus on the primary goal of providing worry-free, dependable service.

13) Has your company secured insurance to cover business losses by yourself or any of your major customers? Has your company secured insurance to cover possible litigation costs and penalties?

There is no planned purchase of insurance specific to Year 2000 compliance.

14) What is your litigation exposure (contractual obligations) if unable to perform due to Y2K compliance failure? What recourse agreements do you have with suppliers?

While there may be some cost of defense should an action be brought against Frontier for Y2k failures, generally our tariffs would insulate us from the damages. With respect to hardware/software areas, absent any specific y2k warranty/remedy in the underlying agreements, exposure should be limited to the general warranty remedies of repair or replacement of the hardware/software. Recourse to our suppliers would most likely limited to the general warranty remedies described above. While we have been providing customers with ongoing information about our Year 2000 efforts, we have disclaimed any compliance warranties as a general matter, a position shared by others in our industry sector.. Frontier is now disseminating information under the auspices of the recently enacted Year 2000 Information & Readiness Disclosure Act. The Act is designed to allow open communications between businesses and the public in general about y2k matters without the risk of having the disclosed information used against the information provider in litigation.

15) Will you disclose progress towards completion of your Year 2000 plan on a regular basis that can be monitored? How would any material change be disclosed to shareholders? 8-k's for material change? MD & A in 10-q and 10-k's? Press releases? Your web page?

We have disclosed, and will continue to disclose Y2K plans in our SEC periodic filings -- 10-Qs and 10-K, with a special disclosure section in the MD&A. If there were a "material change" outside the periodic reporting schedule, that would be disclosed on Form 8-K. Disclosure by way of press release or web page alone would not meet the SEC's criteria of "public dissemination of material non-public information".

16) What about network operation between and among carriers?

Our network is connected to many other networks; carriers are dependent on one another to assist in the completion of calls and we believe that most of the carriers with whom we exchange call traffic are also actively addressing Year 2000 issues. Frontier is actively involved in the Alliance for Telecommunications Industry Solutions (ATIS) and is evaluating participation in an ATIS forum supporting industry wide Year 2000 interoperability testing between telecommunication service providers. We believe we are implementing the best procedures available to us to reduce the risk of any network event, and would match our commitment and remediation activities against any of our competitors.

17) What level of risk assessment has Frontier undergone? Have senior level management been involved in this assessment?

As part of our initial inventory and assessment phase, we attempted to determine our exposure to year 2000 failures. Because the public switched telephone network is made up of facilities under the jurisdiction of hundreds of different companies, Frontier is unable to fully assess the level of exposure. We are confident that we are utilizing the best possible industry practices to mitigate these risks and limit any possible interruption in service delivery to our customers. Our assessment indicated that there is risk in 3-5% of the total lines of code in the enterprise. It has also been determined that exposures in electronic equipment exist at the same rate. In the latter case, the best and often the only recourse we have, is to rely on the manufacturer of the equipment. Since these manufacturers are utilized by many if not most of the companies providing telecommunications services, we are confident that their assertions of reliability are accurate and will limit the risk of failure throughout the network.

18) When and what are the most likely Y2K problems that could occur?

Any application that performs any future calculations would be the first to fail if this has not already happened. In Frontier's case, this would be when calculating the end date of a contract based on the start date and duration. Beginning in January 1999, any calculation of a one year contract would be the first function that could experience a failure. It is important to recognize that early failures would appear in the support systems not in network elements and therefore would not be customer impacting.