THE Y2K PROBLEM AND BREAKS IN THE SUPPLY CHAIN:
CAN THE WRATH OF THE BUG BE SQUASHED?

I. INTRODUCTION

As the new millennium approaches, every business must be prepared to answer two very important questions: What impact will the arrival of the year 2000 have on business, and what can, or must, be done to minimize potential problems?

A single computer's failure to recognize the year 2000 may cause it to produce incorrect results or induce the entire computer system to "crash."1 In an era in which daily life has become extremely dependent on computers, what has variously been called the millennium bug, the year 2000 issue, or the Y2K problem, could have "the power to paralyse [sic] the planet."2 This issue will have an effect on every type of organization, from corporations and governmental agencies to the corner store.

"[C]hilling" predictions for January 1, 2000 include: computer failure within the banking system, loss of telecommunications, and loss of electricity.3 Many ponder the question posed by one commentator: "Will the world as we know it end; or will it be an enormous 'non-event'?"4 Until the anticipated date arrives, no one can answer for certain. Predictions of the scope of the problem range from "a global shrink to a temporary meltdown of highly computerized societies."5 An information technology (IT) leader has stated that the Y2K problem "won't send us all to living off roots and grubs ...[b]ut ... you need to be mentally prepared for some bumps in the

---

4Congress introduced a resolution, H.R.J. Res. 14, 106th Cong. (1999), to designate Monday, January 3, 2000 (rather than Friday, December 31, 1999) as the day for observing the New Year's Day holiday in order to give the nation an extra day to deal with problems before heading back to work.
5Michael D. Scott, Year 2000 Update, CYBERSPACE LAW., May 1998, at 27, 28. "Minor headache or major heart attack, at this point it's hard to predict. ... [U]nless the necessary and proper steps are taken immediately by the world's political and business leaders to address Y2K and the interdependencies involved, a major heart attack is the likely outcome." Dean Wayne Rutley, Address at the National Press Club Forum (Aug. 19, 1998), available in LEXIS, Nexis Library, Fed. News Service File (emphasis added).

565
road. Ed Yardeni, a prominent economist working in the Y2K field, believes that the year 2000 problem could "seriously disrupt the entire global economy." He forecasts a seventy percent chance of a global recession as severe as the one caused by the early 1970's oil-supply disruption.

The precise impact that the Y2K issue will have is simply impossible to ascertain, and the potential technical, business, and legal problems are overwhelmingly vast in number. For these reasons, this note is intended to give insight into the Y2K problem and provide a closer look into a particular area of concern for businesses, namely, a breach of contract for the sale of goods caused by Y2K induced supply chain failures. This concern, like many others, will contribute to the price businesses ultimately pay for the turnover into the year 2000. This note, therefore, will also offer some thoughts on how to curb this costly bug.

II. CAUSES, EFFECTS, AND PRELIMINARY MEASURES

The Y2K problem was born of very simple roots. The potential ramifications of the bug, however, are widespread, affecting organizations both internally and externally. These issues, as well as the methods and costs of dealing with the problem, are the subject of this section.

A. The Birth of a Bug

The year 2000 problem stems from the use of a two-digit representation of the year in the date field of many computer programs. For example, the year 1998 is shortened to "98"; 2000 to "00." Computer programmers in the 1960s and 1970s adopted this representation method to

---


8Id.

9For simplicity, this limitation allows analysis under Article 2 of the Uniform Commercial Code.


reduce the costly use of computer memory.\textsuperscript{12} Those concerned with the long-term effects of this practice most likely believed that by the time it would become an issue, systems would be updated with four-digit date fields.\textsuperscript{13}

Unfortunately, this change over did not occur as soon as it could, or should, have. When early hardware was upgraded, users routinely moved existing software from old systems to new ones, "thereby perpetuating the life of code using the two digit year standard beyond original expectations."\textsuperscript{14} Later, new programs were created to function with the existing software, and the two-digit standard "became embedded in the country's installed software base. Thus, adoption of the two digit standard had the inevitable, but unintended, effect of requiring a conversion effort in the future."\textsuperscript{15} And so the millennium bug was born.\textsuperscript{16}

Businesses that have recently upgraded their systems should not simply assume all is well. New hardware and software may also be susceptible to the bug: "Validated systems may not actually be Year 2000-compliant if users have modified them by entering non-compliant data."\textsuperscript{17} Further, even if a business' computer systems are ready for the year 2000, various telecommunications problems may occur as a result of date-sensitive "microprocessors or embedded chips."\textsuperscript{18} Moreover, the scope of the Y2K problem goes beyond personal computers and could cause the failure of

\textsuperscript{12}Id.
\textsuperscript{13}Id.
\textsuperscript{14}Cooney, supra note 1, at 2. This is the concept of "backward compatibility." New software was developed to be compatible with a customer's existing software. Unfortunately, this created an environment in which the Y2K bug could progress "program by program" into today's modern equipment and software. Douglas Stanglin & Shaheena Ahmad, Year 2000 Time Bomb, U.S. NEWS & WORLD REPORT, June 8, 1998, at 45, 48.
\textsuperscript{15}Cooney, supra note 1, at 2.
\textsuperscript{16}Some software programs may have suffered from the "Year 1999 Bug." Kurt L. Ehresman & Frederic M. Wilf, Separating Reality from Hype: The Legal Ramifications of the Year 2000 Problem, PA. LAW., Sept.-Oct. 1998, at 16. In early computer programs, a series of 9s in the data (e.g., "99999") was an end program instruction, signaling that "no further processing was necessary." Id. Left uncorrected, this instruction may have caused programs to stop running when they reached "99" in the year field. Id.
\textsuperscript{18}See id. ("This could affect credit card readers, automatic teller machines, fax machines, pager and e-mail service.").
almost anything with built-in computer microchips. The potential sources of the bug are endless.

B. Effects of the Bug

1. What it Means to be "Compliant" and the Technical Consequences of Noncompliance

Unfortunately, there is not a "generally accepted definition of Year 2000 compliance. Products that are Year 2000 compliant standing alone may not be capable of exchanging data because there are multiple methods of achieving Year 2000 compliance." Aside from the different methods employed to become compliant, a preliminary issue is discerning just what it means to be compliant. Two commentators have noted that the closest we have to a standard definition can be found in the Federal Acquisition Regulations:

Year 2000 compliant ... means ... that the information technology accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations, to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it.

The source of the problem has been described as "ridiculously petty, but in the uncompromising world of computers, it can lead to a host of calculation errors and equipment crashes." Problems will occur in programs that compute calculations involving dates on and after January 1, 2000. A simple example is a program that calculates one's age by

---

19See Cordes, supra note 6, at 1A ("A growing concern is failure of the computer microchips built into all kinds of electronic machines — from household appliances, electric, gas and water systems, industrial machinery, communications networks, life-saving medical equipment and even cars.").
21Klein & Swanson, supra note 3, at 22.
23Dunn, supra note 5, at A1.
24Takach, supra note 11.
deducting the year of birth from the current year. Assuming that the program utilizes a two-digit date field, if you were born in 1965, then in 1990 the program would have calculated your age to be 25 (90 - 65). In the year 2000, however, the same program would compute your age to be -45 (00 - 65).

2. Internal Infestation

Year 2000 failures can occur anywhere computers or software are used, such as purchasing and supply operations or delivery systems. Possible consequences of a Y2K failure include incorrect cancellation of orders and shipments of goods, or entire customer accounts, as well as the malfunctioning of electronic data interchange (EDI) systems and assembly lines.

All businesses are susceptible to the wrath of the bug. It is erroneous to assume that only technological businesses will be affected. The Y2K bug is a systematic problem: software controls telephone systems; businesses relying on just-in-time inventories probably use computers to manage them; and embedded chips are likely to be found in the security systems of many companies. This is "[n]ot to mention all the programs and chips in [a business'] supply chain."

Indeed, even Y2K compliant organizations "may ... confront serious obstacles if important suppliers and service providers fail [to become Y2K compliant]. The Tactical Strategy Group, Inc. recently observed that '[m]ost industries are focused solely on resolving internal year 2000 problems and are ignoring third-party risk factors that could be much more devastating."

Some businesses are just beginning to face the realization that "the Y2K crunch in many ways is beyond their control. It's not enough to solve your own Y2K problems if the power goes out, you have no dial tone or your most important supplier or customer is bitten by the bug." Thus, even

25 Id.
26 Id.
27 Id. Of course, if the program recognizes only the absolute value of a given number, the result will be 45. Id.
30 Klein & Swanson, supra note 3, at 20.
31 Id.
32 Id.
34 Cordes, supra note 6, at A1.
though a business may have its own computer systems in order, the Y2K problem may still affect them through external sources.

3. Breaking Links: Other Businesses' Bugs

Simply declaring that an entity "will be compliant" minimizes the problem and ignores — deliberately or otherwise — the interconnectedness of all systems. 'Compliance', in the face of the level of our dependence on critical infrastructure, is an illusion. It's like kicking the tires of a car and declaring that the vehicle is in working order.\(^{35}\) Businesses are interrelated through their "customers . . . suppliers; vendors; financial service providers; insurance carriers; . . . government agencies; electric utilities; telecommunications networks; and even competitors.\(^{36}\) All it takes is one link in the chain to falter and the entire system is at risk.\(^{37}\)

One particular Y2K problem that has not received the attention it deserves is "a breakdown in the supply chain."\(^{38}\) Two important supply chain "efficiency initiatives" that increase susceptibility to other businesses' bugs are (1) utilization of just-in-time (JIT) inventories\(^{39}\) and (2) a high degree of automation, such as the use of EDI systems to communicate with business partners\(^{40}\) and "automating the factory floor."\(^{41}\) With this increased


\(^{37}\)Id.

\(^{38}\)Rutley, supra note 4.

\(^{39}\)Blaise Zerega, Y2K Bites the Supply Chain, INFOWORLD, Aug. 24, 1998, at 59, 59. With JIT inventory, a business relies on vendors to "supply raw materials on short notice — a move that saves inventory control costs and pushes the actual inventory costs off [its own] financial books and up the supply chain to suppliers." Id. Even if a manufacturer is internally ready, if its JIT supplies do not show up as expected, its production floor may "grind to a halt." Klein & Swanson, supra note 3, at 23. "A manufacturer of TV's, for instance, won't be able to get the supplies and won't have anything in stock." Walsh, supra note 2 (quoting Ken Lindup, senior consultant in information security at SRI Consulting).

\(^{40}\)Zerega, supra note 39, at 59.

\(^{41}\)Any computer users have networked their systems with suppliers, customers, and business partners. A company's efforts to remedy its Year 2000 problem may be frustrated if firms with which it shares data fail to act. The sheer number and complexity of interfaces between various programs in a computer, and between computer systems themselves, are what make Year 2000 correction efforts so difficult.

Cooney, supra note 1, at 2.

\(^{42}\)Nadler & Kirsch, supra note 20.
interdependence between suppliers and manufacturers, a single company's Y2K failure "could have a domino effect" on the supply chain. Thus, even if businesses have exterminated the Y2K bug within their factory and office walls, many may nevertheless suffer from supply chain problems.

C. Coping with the Wrath of the Bug

As the effects of the millennium bug on a particular organization flow both internally and externally, a brief discussion of how businesses are dealing with these issues and the price they are paying is warranted.

1. Internal Extermination

Fixing the problem has been described as "not particularly technical, just tedious." "There is no magic fix that effortlessly can find all [of the problematic date-related codes in programs] and transform them into a four digit presentation." For most software programs, it will be necessary to invest both time and money into the tedious task of checking the program code line-by-line in order to find and correct every problematic date field.

As long as new systems can meet the demands of old noncompliant ones, and the investment is financially feasible, businesses will certainly consider upgrading to Y2K compliant replacements.

Businesses should be aware, however, that any equipment containing embedded computer chips which use a date or calendar record are at risk of

---

42 Id.
43 Id.
44 Cordes, supra note 6, at 1A. [And although no one piece by itself is particularly large, ... there are so many little pieces — billions of programs and microprocessors — that even small adjustments in defect rates, average repair costs and numerous other variables can have a huge impact. The point is that with enough dust, even a little problem can be shoveled into a stratospheric heap. Dunn, supra note 5, at A1.
45 Takach, supra note 11.
46 "Original estimates of $1.00 per line of code to undertake Y2K conversion are constantly being revised upwards as the Y2K deadline looms ever closer and the shortage of trained personnel grows more dire." Id.
47 Id. "Experts estimate that for 10 million lines of code you can expect 300,000 or more dates: 75,000 or more will need expansion, 50,000 or more will be involved in computation, and 1,400 [new] defects will be introduced." Larry Shoup, Managing the Risk of Year 2000: How to Protect Your Organization from Over Spending, Failure and Litigation (visited Oct. 10, 1998) <http://www.year2000.com/archive/janis.html>.
48 Takach, supra note 11.
Y2K failure.\textsuperscript{49} Thus, for many businesses, "[t]he real problem . . . will be the tremendous amount of work necessary to determine whether their computer software and hardware is or is not Year 2000 compliant.\textsuperscript{50}

2. Dealing With Business Partners' Bugs

Preventing internal Y2K failures is only part of the challenge.\textsuperscript{51} Businesses must identify Y2K-vulnerable business partners by gathering information from them regarding their own efforts to achieve Y2K compliance.\textsuperscript{52} Among other things, this would allow businesses to ensure secure contracts and create contingency plans to avoid breaching their obligations. In addition, such information gathering will help "prepare for possible Year 2000-related litigation by and against the company."\textsuperscript{53}

Erroneously assuming that service and product suppliers will be unaffected by the year 2000 problem could be disastrous.\textsuperscript{54} Results from a Securities and Exchange Commission (SEC) readiness report are not reassuring: in an evaluation of 1023 companies, the SEC found that only forty-nine percent had plans to evaluate the Y2K readiness of material business partners.\textsuperscript{55} The Y2K bug is a management problem that must be evaluated by top officials of all companies to ensure that their suppliers will not adversely affect operations.\textsuperscript{56}

Accordingly, manufacturers have taken various approaches to solving their potential supply chain problems. Some have focused on asking for Y2K compliance statements from key suppliers, while relying on "trust and good faith" from less critical suppliers.\textsuperscript{57} Other manufacturers believe that an "in-depth audit" may be necessary for their major suppliers.\textsuperscript{58} A more aggressive approach is to set deadlines for supplier compliance, after which the manufacturer will consider alternative vendors.\textsuperscript{59}

\textsuperscript{49} Hochberg, supra note 17.
\textsuperscript{50} Ehresman & Wilf, supra note 16, at 17.
\textsuperscript{51} Goldberg, supra note 29.
\textsuperscript{52} Id.
\textsuperscript{53} Id. See also infra Part IV.A.
\textsuperscript{54} Meador & Freeman, supra note 36.
\textsuperscript{55} Zerega, supra note 39, at 59-60.
\textsuperscript{56} Rutley, supra note 4, \S 38.
\textsuperscript{57} Zerega, supra note 39, at 60. Lou Marcoccio, the year 2000 research director of the Gartner Group, Inc. in Stamford, Conn., warned that requesting compliance statements may not work because only 20% of Y2K surveys make it back to companies, and only 3% of those are accurate. Kathleen Melymuka, \textit{Will the Chain be Unbroken? Up and Down the Supply Chain, Year 2000 Compliance is Off to a Dismal Start}, \textit{Computerworld}, Mar. 9, 1998, at 76, 80.
\textsuperscript{58} Zerega, supra note 39, at 60.
\textsuperscript{59} Id.
3. Costs of the Bug

The costs of fixing the Y2K problem in the United States alone has been estimated at $300 to $600 billion. The Federal Reserve has projected that the nation's businesses may spend more than $50 billion to get rid of their bugs.

The skill to remediying Y2K problems in computer systems "is already at a premium and will become even more scarce as the new millennium approaches." As a result, many businesses will fail to become compliant, those that do not fail will become anxious to hold others responsible for any Y2K-induced losses. This environment will necessitate legal advice as to "rights, remedies and obligations," as explored in the next section.

III. COURTROOM INFESTATION

Lawyers will "come out of [the Y2K problem] beautifully. . . . There will be hundreds of thousands of . . . cases. The scope is so broad that it's going to be paralyzing." Many firms expect the arrival of the year 2000 to be "a significant revenue generator," with attorneys preparing for litigation resulting from millennium bug problems. Gartner Group, Inc., a business and IT consulting firm in Stamford, Connecticut, has estimated that punitive and compensatory damage awards relating to year 2000 problems may reach $1 trillion — much more than the cost of fixing the problem itself.

The following sections will provide a brief overview of legal issues likely to arise as a result of the Y2K problem. In addition, the issues raised

---

60Cooney, supra note 1, at 2 (citing a projection by the Gartner Group). "[I]ndustry and government will spend enormous sums to upgrade computers that are essential to public safety and the health of the economy." Id. at 1.
61Cordes, supra note 6, at 1A.
62Takach, supra note 11.
63See Shoup, supra note 47 (stating that "[I]ndustry pundits are predicting that 30% of companies will fail to become fully Year 2000 compliant and suffer severe financial consequences, with 1-3% of them declaring bankruptcy"). See also Robert E. Feidler, Beyond the Quill: The Y2K Problem: It Means More Bankruptcies, AM. BANKR. INST.J., July/Aug. 1998, at 36, 37 (stating that the Y2K problem may be "a precipitating cause of bankruptcy in a number of business failures").
64Takach, supra note 11.
65Id.
66Dunn, supra note 5, at A1 (quoting Brian P. Parker and crediting him with filing the first Y2K lawsuit in the United States in June 1997).
68Dunn, supra note 5, at A1.
69See supra text accompanying notes 60-61.
by a breach of contract for the supply of goods caused by Y2K induced supply chain problems will be explored.

A. General Legal Issues

Compounding the inherent problems of the Y2K issue is the fact that lawyers are counting on an abundance of litigation.70 The arrival of the year 2000 may bring with it a swarm of litigants.71 Consumers of computer products may have claims such as fraud or negligence in the design of software72 against software developers, as well as those that supply or license such products.73 In addition, there may be shareholder actions against company directors and officers for failing to prepare for the year 2000.74 Finally, contractual relationships75 may also be at stake. Failures to deliver goods and supplies under contracts due to the millennium bug are among the examples of Y2K problems "likely to spark a raft of civil lawsuits."76 Accordingly, the focus of this note is a breach of contract for the supply of goods caused by Y2K-induced supply-chain failures.77

70Shoup, supra note 47. "[Lawyers] are already lining up for litigation and hope to cash in on the business of finding those who are responsible for failed systems and businesses and prosecuting them to the fullest extent." Id.

71"The possibilities are endless.... [The year 2000 problem] has created a liability equation that sets a potentially unlimited pool of plaintiffs against a universe of potential blame." Dunn, supra note 5, at A1. In fact, several lawsuits have already been filed, although these have primarily been limited to disputes arising from software problems. For a Y2K-lawsuit-tracking resource of filed complaints and case updates, visit <http://www.2000law.com/html/lawsuits.html>.

72Takach, supra note 11. The most difficult task in a negligence of software design case may be "determining the earliest date by which system developers knew, or ought to have known, about the Y2K problem such that not making their systems Y2K compliant henceforth would constitute negligence?" Id.

73Dunn, supra note 5, at A1. Directors and officers may have fiduciary duties "to exercise due diligence to investigate and disclose potential Year 2000 problems." Goldberg, supra note 29. When dealing with potential director and officer liability, businesses are warned not to forget their relationships with business partners. See, e.g., Klein & Swanson, supra note 3, at 35 (stating that a business should "maintain a record of what it has done to ensure Year 2000 compliance (especially of third-party suppliers)"); see also Valdis Krebs, Year 2000 Network Effects (visited Oct. 8, 1998) <http://www.orgnet.com/y2k.html> ("Auditing the Y2K effects of your mission critical business processes and supply chain provides evidence of due diligence when the lawyers come calling.").

74Dunn, supra note 5, at A1.

75See supra text accompanying notes 9-10. One obvious contract issue includes failure to deliver goods because of the supplier's own Y2K problems. See Cohn & Wittman, supra note 10, at 38 ("Unless there is language in existing or new contracts addressing and excusing performance for Y2K specifically, there is no underlying legal theory that will excuse performance of a supply contract by a supplier because of an internal breakdown in the supplier's systems relating to the Y2K issue." Id. (emphasis added)).

Other contract issues involve delivering goods in breach of an unexcluded and unmodified
The extent of legal liability under contract that the Y2K problem will impose on a particular business will be unknown until after January 1, 2000. Therefore, it goes without saying that "much will depend on the specific facts of each case." A general example of contractual problems caused by third-party suppliers is as follows: Come January 1, 2000, a company's internal systems are all working properly. A supplier, however, "didn't fare as well," and the JIT shipments expected by the company never left the supplier's factory. "Tomorrow, [some of the company's] plants will shut down for want of that part. [The company's] JIT shipments to [its] biggest customer won't happen, causing [its] customer to default on an important... contract.

There is little doubt that such cases will arise. First, "many businesses... aren't going to be ready in time. ... [A]s many as half of all small business are not planning to do anything at all." Some of these businesses are bound to be someone else's suppliers. Furthermore, many businesses are simply counting on their suppliers to be capable of fulfilling their contracts as promised. When businesses rely on noncompliant suppliers that fail to deliver, causing breaches of contracts with their buyers, the question of who will be responsible for paying for the damages will be at issue. This question will be quickly posed especially where there are significant damages or where there is a lack of a long-term relationship between the business and its customer. It should be clear that the issue with implied warranty of merchantability or fitness for a particular purpose (e.g., delivering computers which, because they are not Y2K compliant, may not be "fit for the ordinary purposes for which [computers] are used", see U.C.C. § 2-314(c), 1A U.L.A. 212 (1989), and/or may not be fit for a particular purpose when the seller should know "that the buyer is relying on the seller's skill" to supply goods for such purpose, see U.C.C. § 2-315, 1A U.L.A. 380 (1989)). Analysis of these and other issues is beyond the scope of this note.

Takach, supra note 11.

Meador & Freeman, supra note 36.

Id.

Id.

Cordes, supra note 6, at 1A.

Melymuka, supra note 57, at 76. "'The vendor issue is the biggest risk issue and the biggest litigation risk issue and the issue people have the least control over, ... [a]nd yet it's where people are focusing the least amount of attention. It makes no sense whatsoever.'" Id. (quoting Lou Marcoccio, year 2000 research director at Gartner Group, Inc. in Stamford, Conn.). Of course, some businesses are not operating with blinders on and are taking steps now to alleviate these risks. See supra text accompanying notes 57-59.

Ehresman & Wilf, supra note 16, at 18.

Takach, supra note 11.
fenontecchnical goods is "not that the good... is compliant, but that the supplier will be there, fulfilling the contract" when the year 2000 arrives.65

The sections that follow provide a look at two particular issues that may arise in a case similar to the one described above: the allocation of the risk of supply-chain failures through contracted warranties and conditions, and a possible defense.

1. Assigning the Risk of a Failure in Supply:

Warranties and Conditions

With the approach of the next millennium, businesses have been encouraged to review contracts with their business partners to determine the obligations and liabilities of each regarding problems induced by the year 2000.68 This assessment should include preparing for potential problems caused by supply chain failures.69 Year 2000 compliant manufacturers concerned with breaching contracts with third parties because of their own noncompliant suppliers' failures90 should consider obtaining warranties from those suppliers.91 Warranties against Y2K-induced delivery failures should be secured, either by requiring such warranties in new contracts92 or by modifying existing contracts.93 This takes care of the source of the compliant manufacturer's breach94 of contract with the third party by

65Klein & Swanson, supra note 3, at 23, 35.
66See supra text accompanying notes 79-81.
67Ehresman & Wilf, supra note 16, at 18.
68See supra notes 54-56.
69Again, such a problem may occur where the compliant supplier utilizes "just-in-time inventory." See Zerega, supra note 39, at 59.
70For an example of a warranty of product compliance that may be considered between licensors and licensees of software, see Timothy J. Feathers, Year 2000 Warranty (visited Oct. 10, 1998) <http://www.year2000.com/archive/warranty.html>. For a discussion of warranties and the Y2K problem in the merger and acquisition setting, see Brette S. Simon, A Lesson in Representations, Warranties, and Indemnities, BUS. LAW TODAY, Sept.-Oct. 1998, at 42, 42. Again, these issues are among those beyond the scope of this note.
71"New contracts should clearly assign responsibility for Year 2000 compliance..." Goldberg, supra note 29.
72Note that in a contract for the sale of goods, no new consideration is necessary for a modification to be binding. U.C.C. § 2-209(1), 1 U.L.A. 417 (1989). If the modification consists of a change in each party's obligations, see infra note 128 and accompanying text, then a consideration issue does not exist.
73Commentators have suggested that companies obtain warranties of Y2K "preparedness" from key suppliers. Klein & Swanson, supra note 3, at 23. The sweeping language of a sample warranty is as follows: "Provider warrants that it shall be able to fulfill all of its obligations under this agreement with no degradation in performance due to the calendar change from 1999 to 2000 and beyond Jan. 1, 2000." Id. at 35.

For reasons discussed below, this cannot be the end of the cyclical story: a statement of
ensuring the manufacturer's rights and remedies against its supplier. Problems remain, however, when the compliant manufacturer steps into the role of supplier to the third party. A "failure of supply" argument as a defense to a breach of contract, absent an express provision in the parties' contract, will likely fail.\footnote{See Cohn & Wittman, supra note 10, at 38 ("A number of legal theories may be advanced where there is an 'upstream' supply-chain breakdown relating to the Y2K issue. Unless there is language in an existing or new contract relating to 'a failure of supply,' using these theories will be very difficult."). Id. The authors do not explain what compromises the "number of legal theories [that] may be advanced" by the breaching party. Id. One possibility is a defense of impracticability. See infra Part III.B.2.} Hence, the effects of the Y2K problem will trickle down the stream of supply and, left unchecked, will place liability risks on those businesses that have invested the time and money to ensure that their internal operations will be running smoothly on January 1, 2000.

There is some hope, however, that compliant manufacturers will reach a mutually beneficial agreement with buyers before such a situation arises. Customers will be concerned with suppliers delivering goods as promised, while suppliers will be concerned with their customers fulfilling notification and payment requirements that may depend on having compliant equipment and computer systems.\footnote{Cohn & Wittman, supra note 10, at 38. See also U.C.C. § 2-301, 1A U.L.A. 8 (1989) ("The obligation of the seller is to transfer and deliver and that of the buyer is to accept and pay in accordance with the contract.").} Due to the bilateral nature of the problem, suppliers may be in a superior bargaining position to protect themselves from liability resulting from a breach of contract caused by supply-chain failures.\footnote{See infra Part IV.A.1 (discussing the importance of cooperation in alleviating the effects of such problems).} A supplier may attempt to completely shift the risk of a supply-chain failure to its buyer, if the parties expressly provide for such a condition in their contract.\footnote{A condition is an event, not certain to occur, which must occur, unless its non-occurrence is excused, before performance under a contract becomes due. RESTATEMENT (SECOND) OF CONTRACTS § 224 (1981).} Such a provision might provide that the seller's duty to deliver goods under contract is conditioned on the seller receiving from its suppliers, without interference caused by the Y2K problem, the inputs necessary to produce and deliver such goods. In such a provision, the condition that must occur is actually a nonevent: the Y2K problem must not affect the seller's suppliers' ability to perform their contractual duties with the seller.
2. Impracticability

One expected defense to a breach of contract caused by the year 2000 is that the arrival of the millennium is an "act of God." Rest assured, more than one lawyer will be arguing that a vendor could not have foreseen the problem and is not responsible as the judicial system struggles to interpret contracts that were drafted before the year 2000 problem was recognized.

Article 2 of the Uniform Commercial Code allows a seller to be excused for changed circumstances if it is established that the agreed performance is rendered impracticable by the failure of a basic assumption on which the parties' contract was made. For example, a seller in breach may argue that an unanticipated event has occurred, such as a failure of its suppliers to deliver because of Y2K problems, making delivery impracticable or impossible. Therefore, the seller would argue it should be excused for nondelivery or any delay in delivery. This section discusses the impracticability argument in two contexts: when the parties have agreed to a specific source of material for the goods and when they have not.

When the parties have agreed that the seller obtain its supplies from a specifically identified source and that source later fails, the seller may be excused. For example, consider a contract requiring widgets to be made with parts from Company A. Company A then fails to supply these parts to the seller due to Y2K problems. In this situation, the seller will be excused for failing to deliver the widgets, as long as the seller "'(1) employed all 'due measures' to assure that . . . [Company A] would perform, and (2) turned over to the buyer any rights against the supplier corresponding to the seller's claim of excuse." If the seller did not contract with Company A but,
instead, merely relied upon this supplier to provide what the seller needed, then the seller failed to use "all due measures to assure himself that his source... [would] not fail." Requesting adequate assurances that, despite the Y2K problem, the supplier's performance will not be impaired, may provide evidence of such "due measures" and may leave the buyer in a stronger position to enforce the rights which have been turned over to it by the seller.

On the other hand, the seller's breach may arise in a case where no particular source was agreed upon. The seller, in order to be excused, must show that (1) the Y2K-induced failures of the seller's suppliers amounts to a failure of a basic assumption on which the parties contract was made and (2) these failures have rendered the seller's performance impracticable. As previously noted, without an escape clause to this effect in the parties' contract, the argument for the seller will likely fail.

The problem with the first element lies in the fact that the risk of a supply failure normally falls on the seller. The arrival of the year 2000 is hardly an unanticipated event. Considering all the attention given to the Y2K problem, manufacturers should now be aware that such risks exist. This is particularly so when these businesses have themselves undertaken to become Y2K compliant. This argument may carry some weight if, at the time the contract was made, the seller had no reason to know of these risks. The issue is one of timing: at what point did the manufacturer have reason to know that Y2K failures of its suppliers could affect its ability to fulfill contractual obligations? Presumably, that point in time would be when the manufacturer realized its own Y2K problems could affect that ability.

The second element, requiring the seller's performance to be rendered impracticable by the Y2K-induced supply problems, will be difficult to

---

106 See id. § 2-609, 1B U.L.A. 161 (stating the duty not to impair a party's expectation of full performance and providing the right to "demand adequate assurance of due performance" when "reasonable grounds for insecurity arise").
107 Id. § 2-615(a), 1B U.L.A. 195.
108 See supra note 95 and accompanying text. See infra Part III.B.1 for a discussion of escape clauses in this context.
109 See supra note 102.
110 See RESTATEMENT (SECOND) OF CONTRACTS § 266(1) (1981): Where, at the time a contract is made, a party's performance under it is impracticable without his fault because of a fact of which he has no reason to know and the non-existence of which is a basic assumption on which the contract is made, no duty to render that performance arises, unless the language or circumstances indicate the contrary.
meet when the source is not agreed upon. Depending upon the types of goods involved and the response to the Y2K problem of the manufacturers that produce the inputs for those goods, the Y2K problem may induce supply shortages that lead to a temporary decrease in the supply of, and a corresponding increase in the market price of, those inputs. Increased cost to perform does not alone render the seller's performance impracticable. But "a severe shortage . . . of supplies due to a contingency such as . . . [an] unforeseen shutdown of major sources of supply or the like, which either causes a marked increase in cost or altogether prevents the seller from securing supplies necessary to performance," is within the excuse provision of Article 2. The resolution of this issue may turn on whether the increased cost, and thus the effects of the year 2000 on the seller's supply effort, will be considered to have been "due to some unforeseen contingency which alters the essential nature of the performance."

Regardless of whether the parties agreed upon a specific source of materials for the goods, the seller's inability to deliver will likely be only temporary. Assuming the breach is excused, the seller must notify the buyer of any nondelivery or delay. If the delay is "material or indefinite," the buyer may opt to either terminate or modify the contract or await performance. If the buyer fails to "modify the contract within . . . thirty days[,] the contract lapses with respect to any deliveries affected."

IV. MINIMIZING THE DAMAGE

The year 2000 problem "has gone beyond blame." Businesses must "put aside differences and develop new ways to work together." The problem will not be fixed by "everyone sticking their head in the sand. And it cannot be solved by everyone running out to sue." The remainder of this note discusses two ways through which the negative impact of the Y2K problem may be diminished: the initiatives of businesses within the supply-chain and proposed and enacted Y2K related legislation.

\[1^{12}\] Again, the outcome of disputes will often turn on the specific facts of each case. See supra text accompanying note 78.
\[1^{13}\] See supra text accompanying notes 7-8.
\[1^{15}\] Id.
\[1^{16}\] Id. § 2-615(e), 1B U.L.A. 195.
\[1^{18}\] Id. § 2-616(2), 1B U.L.A. 214.
\[1^{19}\] Hearing Before Subcomms., supra note 35.
\[1^{20}\] Id.
\[1^{21}\] Rutley, supra note 4.
A. Inside the Supply Chain: Cooperating and Planning Ahead

The objectives of "a viable Y2K supply-chain" include avoiding wasteful legal costs for all parties, encouraging cooperation, and discouraging parties from trying to shift the risk along the supply chain. Companies that plan for external Year 2000 problems by working with their trading partners while there is still time to adjust contract terms and develop contingency plans will be in the best position to maintain operations and avoid or reduce liability exposure.

1. Cooperation Between the Links

"We either all make this together, or we'll all suffer together."\(^{124}\)

Although the year 2000 is fast approaching, there is still time "to come to grips with this problem for all of us individually, [and] to work together communally on fixing the problem."\(^{125}\) Businesses should heed this advice because the effects of the Y2K problem will permeate throughout the supply-chain, making it difficult to take a hard-lined approach.

The bilateral nature of the problem\(^{126}\) will have a "moderating effect on strategic business and legal proposals advanced to address this issue and should force the participants in a supply chain to search for a fair and reasonable balance."\(^{127}\) This moderating effect may result in an agreement between parties to a contract, whereby each "take[s] on the risk that the subcontractors of the other party will not interrupt the supply of goods or services between the [parties] because of Y2K noncompliance."\(^{128}\)

Some businesses that have achieved Y2K compliance are expected to "'fortress' against those who have not," leaving "'the Y2K barbarians . . . to die outside of the fortress wall.'"\(^{129}\) While the threat of losing customers and being left "'to die'"\(^{130}\) will motivate companies to achieve compliance, the goal

\(^{122}\)Cohn & Wittman, supra note 10, at 38.
\(^{123}\)Goldberg, supra note 29.
\(^{125}\)Yardeni, supra note 7 (emphasis added).
\(^{126}\)See supra text accompanying notes 96-97.
\(^{127}\)Cohn & Wittman, supra note 10, at 38.
\(^{128}\)Id. at 38-39. For a "proposed wording" of such a contract provision, see id. at 39.
\(^{129}\)Feidler, supra note 63, at 36 (quoting Dr. Edward Yardeni, chief economist of the Deutsche Bank Securities).
\(^{130}\)Id.
of business activity in this area should be to gain reassurance that the Y2K problem will not disable businesses from meeting their contractual obligations.\textsuperscript{131}

Customers that request contracts to "warranty Y2K\textsuperscript{132} have been accused of intending to shift the blame.\textsuperscript{133} Rather than shifting risks and pointing fingers, a cooperative solution for minimizing costs of the Y2K problem is exemplified by the Chemical Manufacturers Association (CMA).\textsuperscript{134} The CMA, working with the Center for Dispute Resolution, has drafted an alternative dispute resolution commitment form signed by thirty-five companies pledging "to first pursue mediation rather than litigation in trying to resolve issues" associated with the Y2K problem.\textsuperscript{135}

2. The Importance of Planning

While cooperation with business partners will help minimize the damage of the bug, businesses must have a back-up plan.\textsuperscript{136} Although contingency plans are a business strategy and not a legal requirement, there are two reasons why they are so important with the year 2000 approaching.\textsuperscript{137} The first involves customer-supplier links in the supply chain that are unable to explicitly agree on assuming the risk that Y2K problems might prevent each party from fulfilling contractual obligations. In such a case, contingency planning provides a mechanism whereby the party whose own suppliers have failed may still be able to achieve performance and perhaps avoid legal liability.\textsuperscript{138} Second, when a cooperative agreement has been

\textsuperscript{131}Cohn & Wittman, supra note 10, at 38.

\textsuperscript{132}RV, Companies Conducting Y2K Reviews, Developing Contingency Plans, CHEMICAL WK., Aug. 19, 1998, at 50.

\textsuperscript{133}Id.

\textsuperscript{134}Id.

\textsuperscript{135}See id. (noting that the commitment pledge and list of participating companies can be found on the CMA's web site <http://www.cmahq.com>).

\textsuperscript{136}William Ulrich, How to Solve the Contingency Planning Problem, COMPUTERWORLD, Aug. 17, 1998, at 27, 27. A study through mid-1998 found that companies performing contingency planning for the year 2000 had increased from 3% to 72%, indicating that they "now realize their best efforts can't eliminate all year 2000 problems." Id.

\textsuperscript{137}Contingency plans for supply problems are certainly not a new idea. For example, in the health care industry, "[a] break in supplies is something clinics always anticipate as part of normal contingency planning." Melymuka, supra note 57, at 77. For supply-chain links with single-source suppliers, contingency planning for supply-chain failures is not an option. When a business relies on such suppliers, it may have to consider doing the Y2K remediation for them. Zerega, supra note 39, at 60. Where switching vendors is feasible, there remains the problem of receiving assurances that the new supplier will be able to deliver without disruption caused by its own internal Y2K problems. Id.

\textsuperscript{138}See supra text accompanying notes 96-98, 126-28.
reached and a supply-chain failure occurs, a healthy contingency plan will facilitate the performance that the parties originally agreed to, thereby ensuring smooth business operations.\textsuperscript{139}

B. Legislation: Friend or Foe?

With attention on the millennium bug increasing as the days to the deadline dwindle, a number of states and the federal government have been prompted to address the issue with various legislative responses. These include "sovereign immunity legislation," "litigation-related legislation,"\textsuperscript{140} and legislation generally aimed at facilitating the elimination of the Y2K problem.

Five states have passed sovereign immunity bills to shield themselves from liability relating to the Y2K problem.\textsuperscript{141} Nevada was the first\textsuperscript{142} to pass such legislation, which generally precludes actions against the state on the basis of a Y2K problem.\textsuperscript{143} Nevada's statute additionally requires that

[a]ny contract entered into by or on behalf of . . . the State of Nevada, an immune contractor or an officer or employee of the state . . . must include a provision that provides immunity to those persons for any breach of contract that is caused by an incorrect date being produced, calculated or generated by a computer or other information system that is owned or operated by any of those persons, regardless of the cause of the error.\textsuperscript{144}

\textsuperscript{139}Hochberg, supra note 17. Businesses are encouraged "to develop contingency plans for keeping their businesses operating" because vendors and other contacts may not be Y2K compliant. \textit{Id.} Contingency plans are important because a break in the chain caused by one supplier's Y2K problems "could have a domino effect throughout the industry." RV, \textit{Companies Conducting Y2K Reviews}, supra note 132, at 50.


Presently, there is "no talk" of federal-level sovereign immunity legislation. Dinstein,\textit{ supra} note 140, at 4.

\textsuperscript{142}Dinstein,\textit{ supra} note 140, at 3.

\textsuperscript{143}2 NEV. REV. STAT. ANN. § 41.0321 (Michie 1997).

\textsuperscript{144}\textit{Id.} § 41.0321(2). A provision of any contract entered into after June 30, 1997, which is in conflict with § 41.0321 is void. \textit{Id.} § 41.0321(3).
Such laws are generally aimed at preventing frivolous lawsuits "such as those in which people might blame a backed-up city sewer for their rug stains." ¹⁴⁵ In other words, immunity laws may help thwart the "millennial ambulance chasers." ¹⁴⁶ These laws, however, are not without valid criticism: Reed Kathrein, head of the Y2K team at the New York law firm Milberg Weis, stated that governments "should be making sure [problems] don't happen rather than running around trying to protect themselves without doing their homework. . . And [immunity] certainly does not encourage them to get the job done." ¹⁴⁷

Although statutorily mandated contract provisions may excuse a state from liability for a breach of contract due to the millennium bug, private parties relying on such contracts are precluded from bargaining with "immune contractor[s]"¹⁴⁸ to lessen the risks of supply-chain failures.¹⁴⁹ Instead, private parties will have to resort to contingency planning to minimize the risk of breaching a contract with a third party buyer.¹⁵⁰

A second type of legislation has been proposed with the intention of reducing the "expected flood of Y2K litigation" by limiting causes of action and recoverable damages.¹⁵¹ Bills, such as the one that failed in California¹⁵² and the Dreier-Cox bill,¹⁵³ "seek[] to limit damages by barring punitive damages and limiting plaintiffs to only the actual costs of fixing the problem, as long as the defendant(s) make a good faith effort to fix the problems in time."¹⁵⁴ Damages will be limited as long as the claimant "has not suffered any personal injury . . . as a result of the computer date failure."¹⁵⁵ These bills specifically address concerns of the computer industry by "immun[izing them] from suits for fraud, negligence or unfair

¹⁴⁶Id.
¹⁴⁷Id. Immunity will also not prevent leaders from suffering political "fallout[s]" if they failed to properly prepare for the Year 2000. Id. (citing Jim Cassell, research director of the Gartner Group, Inc., Stamford, Conn.). People will have "one of three words for it: stupid, gutless, or negligent." Id.
¹⁴⁸See supra text accompanying notes 126-28.
¹⁴⁹See supra Part IV.A.2.
¹⁵¹Dinstein, supra note 140, at 3 (referring particularly to A.B. 1710, 1997-98 Reg. Sess. (Cal. 1997), which died in committee). At the federal level, the Dreier-Cox bill, H.R. 4240, 105th Cong. (1998), which also died in committee, was substantially similar in form to the defeated California bill.
¹⁵³See supra note 151.
¹⁵⁴Scott, supra note 4, at 28.
trade practices if they undertook reasonable efforts to correct the problem." Successful legislation of this kind would not preclude claims under contract but, rather, would "cap liability at actual losses for third parties seeking recompense for [Y2K-related] computer problems." 

The recently introduced Y2K Act\textsuperscript{158} addresses many of the same concerns as the Dreier-Cox bill.\textsuperscript{159} The Y2K Act would regulate commerce by providing for the resolution of disputes arising from the Y2K issue.\textsuperscript{160} The Y2K Act would limit damages to economic losses,\textsuperscript{161} except when the parties have contracted otherwise,\textsuperscript{162} and when the plaintiff proves "conscious and flagrant disregard, rather than mere negligence, on the part of the defendant."\textsuperscript{163} In addition, the Y2K Act\textsuperscript{164} would limit damages to economic losses where the defendant has attempted to prevent or remedy a "Y2K failure" with the diligence and care expected of a party in the defendant's line of business.\textsuperscript{165} 

Regarding the sale of goods, this type of legislation would primarily affect cases in which a defendant shipped non-Y2K compliant goods or failed to deliver because of internal Y2K failures.\textsuperscript{166} If passed, the Y2K Act will apply to "any Y2K action."\textsuperscript{167} It follows that the Y2K Act should also apply to cases where the defendant's breach is caused by the Y2K problems of its suppliers. Generally, the bill defines a "Y2K action"\textsuperscript{168} as a civil action "arising out of a Y2K failure."\textsuperscript{169} "Y2K failure" is defined as "a systems product failure caused by the Y2K bug."\textsuperscript{170} Thus, the bill's applicability would not be confined to cases "arising out of" the defendant's own internal Y2K problems.

\textsuperscript{156}State Developments: Cal. Legislature Fails to Act on Y2K Bill, CYBERSPACE LAW., June 1998, at 18, 18.
\textsuperscript{157}Coalition of Interests Want Say in Drafting 'Good Samaritan' Bills, 1 MEALEY'S YEAR 2000 REP., July 23, 1998, at 7, 8.
\textsuperscript{158}S. 96, 106th Cong. (1999).
\textsuperscript{159}H.R. 4240, 105th Cong. (1998).
\textsuperscript{160}S. 96, 106th Cong. (1999).
\textsuperscript{161}Id. \textsection 5(A).
\textsuperscript{162}Id. \textsection 4(A).
\textsuperscript{163}Id. \textsection 5(C)(2). Punitive damages may only be awarded if authorized by state law. Id.
\textsuperscript{164}S. 96, 106th Cong. (1999).
\textsuperscript{165}Id. \textsection 5(D).
\textsuperscript{166}Id. \textsection 2(2). For example, the Y2K Act would require that a plaintiff notify the defendant in writing of any Y2K failures and give the defendant an opportunity to correct the problem before a case would proceed to trial. Id. \textsection 4(B).
\textsuperscript{167}S. 96, 106th Cong. \textsection 3(A) (1999).
\textsuperscript{168}Id. \textsection 2(1) (1999).
\textsuperscript{169}Id. \textsection 2(2) (emphasis added).
\textsuperscript{170}Id. (emphasis added).
An example of the third type of Y2K legislation — legislation generally designed to help exterminate the bug — is the Year 2000 Information and Readiness Disclosure Act (the Act).\(^{171}\) Signed by President Clinton on October 19, 1998, the Act's stated purposes are:

1. to promote the free disclosure and exchange of information related to year 2000 readiness;
2. to assist consumers, small businesses, and local governments in effectively and rapidly responding to year 2000 problems; and
3. to lessen burdens on interstate commerce by establishing certain uniform legal principals in connection with the disclosure and exchange of information related to year 2000 readiness.\(^{172}\)

To accomplish these goals, the Act shields a company from liability for making inaccurate statements regarding its readiness unless the claimant establishes that the "maker" made the statement "(i) with actual knowledge that the year 2000 statement was false, inaccurate, or misleading; (ii) with intent to deceive or mislead; or (iii) with a reckless disregard as to [the statement's] accuracy."\(^{173}\) The Act also creates an evidentiary exclusion "precluding the admission of any 'Year 2000 Readiness Disclosure' against the 'Maker' of the disclosure to prove the accuracy or truth of any Year 2000 statement in such disclosure."\(^{174}\) Another important section provides a temporary and limited antitrust exemption "to promote information sharing between parties who might otherwise be considered competitors."\(^{175}\) The Act does not directly affect the contractual supply-chain issues discussed in this note. If its purposes are served, however, the promotion of cooperation among businesses should help to lessen the existence of Y2K problems.

Another federal bill aimed at facilitating the efforts to eliminate the millennium bug is the proposed Small Business Year 2000 Readiness Act.\(^{176}\) To prevent Y2K failures, this legislation recognizes that the potential


\(^{172}\)Id. § 2(b).

\(^{173}\)Id. § 4(b).


\(^{175}\)Id. (citing Year 2000 Information and Readiness Disclosure Act § 5).

\(^{176}\)S. 314, 106th Cong. § 1 (1999).
negative effects of the year 2000 on small businesses will be exacerbated by insufficient capital. This bill would amend the Small Business Act and require the Small Business Administration (SBA) to establish a loan guarantee program to help alleviate the financial strain on small businesses caused by the Y2K bug. This bill increases the total amount a small business may borrow through the SBA, from $750,000 to $1 million. The passage of this bill would make Y2K loans available to help small businesses along the supply chain attack their internal bugs by updating noncompliant IT systems or by purchasing new ones.

V. CONCLUSION

It is too soon to tell exactly what effect the arrival of the year 2000 will have on the world. What is known, however, is that businesses will be affected both internally as well as externally. Companies may spend billions of dollars fixing the problem and paying off judgments and settlements if preventative measures fail. Legislators are well aware of the ill-fated millennium bug problem as they continue to address Y2K issues. To avoid a potential disaster, all are "[p]repar[ing] for the worst and hop[ing] for the best." The proof of [the] collective efforts [to squash the bug] will be an uneventful New Year's Day in the year 2000, and less extra business for [litigators] . . . in the new millennium."

Holly M. Barbera

177 Id.
179 Id. § 3(A).
180 Id. § 3(a)(D).
181 See supra Part II.C.1. Additionally, this bill would allow small businesses to deduct up to $40,000 worth of computer purchases and software upgrades necessitated by the expectation of the year 2000 as an expense, rather than a deduction of a depreciable asset for federal income tax purposes. H.R. 179, 106th Cong. § 2 (1999).
182 Klein & Swanson, supra note 3, at 20.
183 Id. at 35.