WILMER, CUTLER & PICKERING

e-commerce news

July 21, 1999

Y2K LEGISLATION ALERT

On July 1, 1999, Congress passed the "Y2K Act," which is intended to encourage Y2K remediation efforts and informal dispute resolution while limiting frivolous lawsuits arising out of Y2K failures. The law was transmitted to President Clinton by e-mail (a first in federal legislative procedure), and the President is expected to sign it soon.

The Y2K Act creates important new protections from litigation and liability arising out of Y2K failures, and includes new liability allocation and dispute resolution procedures. However, the Act expressly excludes from coverage a number of significant categories of litigation, includes many limitations and conditions, and contains complexities and ambiguities in terminology that likely will require judicial interpretation. Accordingly, businesses will continue to face significant Y2K liability risks, and should proceed with implementation of Y2K remediation plans and programs intended to reduce or eliminate those risks.

Action Items

Businesses should continue to work on minimizing potential liability for Y2K failures. Here are some suggestions:

- ***Implement a comprehensive Y2K readiness assessment and remediation program.*** The most effective way to avoid potential Y2K-related liability is to prevent Y2K failures. These failures can occur in virtually any software, computer, computer chip, or electronic device that processes date information. Businesses should identify immediately all safety- and mission-critical systems, equipment, and facilities that might in any way be affected by Y2K failures, and to undertake full remediation programs as quickly as possible.

- ***Cooperate and communicate with third parties.*** Interdependencies with business partners, critical suppliers, and customers present a major risk of Y2K failures to many companies. Reducing this risk requires cooperation — sharing information about Y2K preparedness and identifying ways that parties can work together to resolve or minimize the effects of potential failures. In many cases, businesses have entered into Y2K confidentiality agreements, requiring them to hold Y2K-related information confidential and not use that information for purposes of litigation. Businesses also may agree to a number of

additional contractual provisions that will facilitate cooperation and reduce likelihood and impact of disputes. For more information on these contractual options, please request a copy of our "Year 2000 Contract Tool Kit" (January 1999). Finally, businesses should consider developing a Y2K communications program (including web site disclosures), with appropriate input from counsel.

- ***Develop contingency plans.*** Because it generally is impossible to eliminate all Y2K risks, businesses should develop contingency plans to mitigate the effects of any potential Y2K failures that do occur. Contingency plans may include options such as identifying manual work-arounds for automated processes, identifying alternative sources of supply, and maintaining additional inventory during critical transition periods.

- ***Designate a Y2K Transition Director.*** Effective Y2K planning requires a comprehensive, coordinated effort, with support at the highest level of management. Many businesses have designated a Y2K Transition Director to manage effective implementation of this process. Under the Y2K Act, companies will need to identify a Y2K Transition Director or other appropriate official for purposes of receiving prelitigation notices under the Y2K Act.

- ***Prepare for possible litigation.*** While taking all possible measures to avoid Y2K failures, businesses also should take steps to protect themselves in the event that litigation does occur. To help minimize risks of liability, businesses should develop a policy for managing, reviewing, and retaining all documents that may relate to Y2K problems or mitigation efforts. This should include developing a system to record and document potential Y2K disruptions, efforts taken to remediate Y2K problems, and the consequences of Y2K disruptions. Businesses also should design and enforce corporate policies concerning disclosure of Y2K information to third parties with supervision of corporate or outside counsel. Finally, insurance coverage should be evaluated and supplemented as appropriate.

Summary of Key Provisions of the Y2K Act

Scope. The Y2K Act applies to any civil action, in federal and state courts, as well as in proceedings before a government agency board of contract appeal, where (1) "the plaintiff's alleged harm or injury arises from or is related to" a Y2K failure, or (2) "a claim or defense arises from or is related to" a Y2K failure. The term "Y2K failure" is defined broadly to include virtually any failure to accurately process dates in the years 1999-2001. The Act expressly does not apply to actions arising under securities laws, claims for personal injury or wrongful death, and most enforcement proceedings brought by government agencies.

Prelitigation Notices. Before bringing any Y2K action (other than actions seeking injunctive relief only), prospective plaintiffs will be required to send to each prospective defendant a written notice that includes specific detailed information describing (1) the alleged Y2K defects or failures, (2) any harm or loss suffered by the plaintiff, (3) the plaintiff's proposed remedy, and (4) the basis for seeking that remedy. Parties receiving prelitigation notices are required to provide a written response within 30 days describing the actions that have been or will be taken to address the Y2K problem described by the prospective plaintiff. The response also must state whether or not the prospective defendant is willing to participate in alternative dispute resolution ("ADR"). The Act provides that these written statements generally will not be admissible in any federal or state Y2K litigation.

Remediation Period. If a prospective defendant has responded to a prelitigation notice by offering proposed remedies or by agreeing to participate in ADR, then the prospective plaintiff must wait at least 90 days (unless the parties agree to a different

time period) from the defendant's receipt of the notice before bringing suit. If the defendant fails to respond or provides an incomplete response to a prelitigation notice, the plaintiff may bring suit 30 days after the defendant receives the plaintiff's notice. If a plaintiff files a Y2K action prematurely, the defendant may notify the court and request a stay of any judicial proceedings pending the running of the remediation period.

Class Actions. The Y2K Act imposes class action notice requirements that are more stringent than those generally applied under federal court rules, and places two limits on class action suits based on alleged Y2K failures. First, in order to certify a class, state and federal courts must find that the alleged defect would be "material" in relation to the performance of the underlying product or service as a whole. Second, the Act requires plaintiffs to bring proposed class action suits in state courts in certain circumstances (*e.g.*, where the proposed plaintiff class has fewer than 100 members or where the aggregate amount in controversy is less than $10,000,000 and the plaintiffs do not seek punitive damages).

Consumer Mortgages. The Act creates a grace period in which mortgagors may not foreclose on consumer residential mortgages if the consumer defaults after December 15, 1999 and the default was due to a Y2K failure. The defaulting borrower must notify the loan servicer within seven days of learning of the failure and in no event later than March 15, 2000. The statutory grace period lasts for four weeks following the date of the borrower's notice. If the borrower does not make the required payment(s) prior to the end of the grace period, the mortgagor or loan servicer may then begin foreclosure proceedings.

Proportionate Liability. The Y2K Act provides that in covered actions *other* than contract actions (a term not defined by the Act), damages generally will be required to be apportioned among all persons (including non-parties and the plaintiff) that contributed to the plaintiff's loss, and that plaintiffs may recover from each defendant only an amount proportionate to that defendant's share of liability. The proportionate liability provisions are not applicable to (1) non-class action suits brought by consumers concerning defects in consumer products, (2) defendants that acted fraudulently or with the intent to injure the plaintiff, and (3) certain cases where all or part of the judgment against one of the defendants is not collectible (for example, due to bankruptcy or other reasons). The Act also establishes rules for defendants seeking contribution from other responsible persons.

Punitive Damages. Where the underlying law allows the recovery of punitive damages, plaintiffs must prove by clear and convincing evidence that they meet the applicable punitive damages standards. The Act places a cap on punitive damage awards against businesses with fewer than 50 full-time employees and individuals with a net worth of less than $500,000, unless the defendant acted with specific intent to injure the plaintiff.

Duty to Mitigate Damages. Under the Act, plaintiffs will not be entitled to compensation for any damages that the plaintiff could have avoided in light of any information, including disclosures by the defendant, of which the plaintiff was or reasonably should have been aware. This duty does not apply, however, to damages from a plaintiff's justifiable reliance on a knowing, material misrepresentation by the defendant.

Stricter Knowledge Standard for Defendants Indirectly Involved in Y2K Failures. The Act includes additional limitations on suits alleging Y2K failures that are brought against parties who did not participate directly in the relationship or activity that formed the basis for the alleged liability. These provisions apply to suits for money damages where: (1) the defendant is not the manufacturer, seller, or distributor of a product, or the provider of a service, that experiences the Y2K failure; (2) the plaintiff and defendant are not in "substantial privity" (a defined term) with each other; (3) the defendant's actual or constructive awareness of the Y2K failure is an element of the claim; and (4) the claim is not a claim for negligence. In suits that meet these criteria, the Act requires the plaintiff to show, in addition to other elements required to prove a claim, that the defendant "actually knew, or recklessly disregarded a known and substantial risk" that the Y2K failure would occur.

Control as a Basis for Liability. The Act provides that a party's control over the facility, system, product, or component that experienced a Y2K failure may not constitute the sole basis for liability. In some cases, this provision may have little practical effect, because the other elements of liability, such as duty or constructive notice, may be independently demonstrated.

Preservation of Existing State Law. The Act provides that certain elements of Y2K claims or defenses must be decided under the law as it existed on January 1, 1999, effectively preventing states from recognizing certain claims or defenses for the first time in Y2K actions. Examples include the law relating to impossibility or commercial impracticability in contracts and elements of claims involving a defendant's state of mind. The Act also allows states to pass laws providing Y2K defendants with greater protections.

Y2K Upset Defense in Government Enforcement Actions. Under limited circumstances and for a limited time, the Act allows defendants to avoid penalties for "Y2K upsets," defined as the failure to comply with "federally enforceable measurement, monitoring or reporting requirements" due to Y2K failures that are "beyond the reasonable control of the defendant." Defendants may only assert the "Y2K upset" defense if: (1) the noncompliance would not threaten public health, safety, or the environment; (2) the applicable requirement did not involve regulation of securities, or the banking or monetary systems; (3) the noncompliance was not caused by "operational error or negligence"; (4) the defendant made a reasonable good faith effort to prevent the failure; (5) the defendant takes immediate action to correct the noncompliance as soon as the defendant invokes the defense; and (6) the defendant notifies the federal authority within 72 hours of learning of the Y2K upset. The Y2K upset defense does not apply to actions in which the federal agency seeks only an injunction or an order requiring the defendant to comply with the underlying requirement.

Relationship to the Year 2000 Information and Readiness Disclosure Act ("IRDA"). The Y2K Act provides that the provisions of the IRDA shall apply to any Y2K action. The IRDA may limit the admissibility of certain Year 2000 disclosures, but the extent of its protection is unclear. (For additional information on the IRDA, please request a copy of our November 1998 client mailing on that statute.)

What Does This All Mean?

As a practical matter, the protection offered by the Y2K Act likely will be limited. First, the Act does not apply to a number of significant categories of potential Y2K suits, including actions for personal injury and wrongful death. Second, many of the Act's provisions, such as the cap on punitive damages and the proportionate liability provisions, apply only to narrowly defined subsets of Y2K suits. Third, the Act includes numerous terms and provisions that are unclear or ambiguous, making it likely that litigation will be necessary on interpretive issues and creating uncer-

tainty as to the Act's ultimate scope of protection. Fourth, the Act creates new dispute resolution and liability allocation issues that also may contribute to future uncertainty and litigation. Finally, the Act presents a number of potential constitutional questions, including particularly the issue whether it unduly interferes with the states' judicial powers. Thus, while businesses should keep the Y2K Act in mind when designing Y2K remediation programs and otherwise addressing Y2K liability exposure, they should not rely on the Act to shield them from potential liability for Y2K failures.

James R. Wrathall
David M. Kreeger

Monthly Update

Broadband. On July 1, Rep. Billy Tauzin (R-LA) introduced the *Internet Freedom and Broadband Deployment Act* (H.R. 2420), a bill to deregulate the Internet and high speed data services. In addition, Rep. Ed Markey (D-MA) has begun circulating draft legislation that would essentially require cable TV operators to open their broadband networks to access by other ISPs.

CALEA. The House passed legislation (H.R. 916) to alter deadlines and definitions for industry compliance with the *Communications Assistance for Law Enforcement Act.* The bill would extend the phone industry compliance date from January 1, 1995 until June 30, 2000, or beyond. The measure would also extend the "grandfathering" date to June 30, 2000, which would allow phone companies to be reimbursed by the government for changes made to systems installed up to that date.

Database Protection. On June 30, the Subcommittee on Finance and Hazardous Materials of the House Commerce Committee held a hearing on H.R. 1858, the *Consumer and Investor Access to Information Act*, a bill to promote electronic commerce through improved access for consumers to electronic databases, including securities market information databases.

Department of Commerce. The Department of Commerce released their new report, *Falling Through the Net: Defining the Digital Divide*. The President and Secretary Daley released this report as part of the Administration's New Markets Initiatives tour to encourage private sector investment in under-served markets and in high-tech training programs. *Falling Through the Net* underscores the need for greater access to new technologies so that all Americans can gain the necessary skills to compete in our growing digital economy.

Encryption. The House Select Intelligence Committee approved in closed session its version of a bill (H.R. 850) to loosen export controls on technology to encode, or encrypt electronic communications. The bill included a substitute amendment that would allow the export of stronger encryption products than under current policy, after a 45-day technical review.

Internet access. Rep. John Larson (D-CT) introduced H.R. 2534, a bill directing the National Science Foundation to develop a report on the establishment of high-speed, large bandwidth capacity Internet access for all public elementary and secondary schools and libraries in the United States.

and secondary schools and libraries in the United States.

Internet Freedom Acts. On June 30, the House Judiciary Committee held a hearing on H.R. 1685, the *Internet Growth and Development Act of 1999* and H.R. 1686, the *Internet Freedom Act*. H.R. 1685 provides for the recognition of electronic signatures for the conduct of interstate and foreign commerce, to restrict the transmission of certain electronic mail advertisements, to authorize the Federal Trade Commission to prescribe rules to protect the privacy of users of commercial Internet web sites and to promote the rapid deployment of broadband Internet services. H.R. 1686 would ensure that the Internet remains open to fair competition, free from government regulation, and accessible to American consumers.

Privacy/Financial Information. Late July 1, the House of Representatives passed H.R. 10, the financial modernization bill, by a vote of 343 to 86. In the course of consideration, the House approved by a 427-1 vote an amendment by Reps. Mike Oxley (R-OH), Deborah Pryce (R-OH), and Marge Roukema (R-NJ) that would enable customers to opt out of allowing their financial services institutions from sharing personal financial information with third parties. The privacy amendment also prohibits financial institutions from giving out credit card, savings, and transaction account information for marketing purposes. H.R. 10 and S. 900, which passed the Senate on May 6, must now be reconciled by a special Conference Committee that will be composed of select members from each chamber of Congress. For financial modernization legislation to become law, the Conference Committee must agree on a compromise bill that is then separately approved by both the House and the Senate and signed by the President.

Privacy/General. The Federal Trade Commission testified on July 13 before Congress on the status of industry efforts to protect consumers' online privacy. Chairman Robert Pitofsky and FTC Commissioners Sheila F. Anthony, Mozelle W. Thompson and Orson Swindle presented the Subcommittee on Telecommunications, Trade, and Consumer Protection of the House Commerce Committee with a report titled, "Self-Regulation and Privacy Online" (available at http://www.ftc.gov/os/1999/9907/index.htm#13). The report states that "the Commission believes that legislation to address online privacy is not appropriate at this time. We also believe that industry faces some substantial challenges. Specifically, the present challenge is to educate those companies which still do not understand the importance of consumer privacy and to create incentives for further progress toward effective, widespread implementation."

Privacy/Medical information. Rep. John Murtha (D-PA) introduced H.R. 2404, a bill to protect the privacy of individuals by ensuring the confidentiality of information contained in their medical records and health-care-related information.

WCP's E-Group

David R. Johnson	202-663-6868	DJohnson@wilmer.com
Scott Blackmer	202-663-6167	SBlackmer@wilmer.com
Brandon Becker	202-663-6979	BBecker@wilmer.com
Russell Bruemmer	202-663-6804	RBruemmer@wilmer.com
Patrick J. Carome	202-663-6610	PCarome@wilmer.com
Louis R. Cohen	202-663-6700	LCohen@wilmer.com
Susan P. Crawford	202-663-6479	SCrawford@wilmer.com
Stephen P. Doyle	202-663-6282	SDoyle@wilmer.com
Franca Harris	202-663-6557	FHarris@wilmer.com
Andrew Herman	202-663-6422	AHerman@wilmer.com
Samir C. Jain	202-663-6083	SJain@wilmer.com
Mary Kostel	202-663-6896	MKostel@wilmer.com
David M. Kreeger	202-663-6407	DKreeger@wilmer.com
Charles S. Levy	202-663-6400	CLevy@wilmer.com
John B. Maull	202-663-6269	JMaull@wilmer.com
Jeffrey McFadden	202-663-6385	JMcFadden@wilmer.com
John A. Payton	202-663-6325	JPayton@wilmer.com
Daniel Phythyon	202-663-6545	DPhythyon@wilmer.com
James R. Wrathall	202-663-6895	JWrathall@wilmer.com
Soo J. Yim	202-663-6958	SYim@wilmer.com

This memorandum is for general purposes only and does not represent our legal advice as to any particular set of facts, nor does this memorandum represent any undertaking to keep recipients advised as to all relevant legal developments.