WILMER, CUTLER & PICKERING

ECommerce News

August 2, 2000

New Electronic Signatures Law

On July 3, President Clinton signed the Electronic Signatures in Global and National Commerce Act ("E-SIGN"), a statute that establishes the legal validity of electronic contracts, consumer disclosures, and recordkeeping. This key piece of legislation will have dramatic effects on e-commerce.

What does the new law cover? E–SIGN is perhaps best thought of as the "No-Paper-Needed Act." It authorizes the use of electronic means instead of paper to meet legal requirements in three broad areas: electronic contracts and signatures, consumer disclosures, and recordkeeping.

- **Electronic Contracts and Signatures**. The heart of the new law is a preemptive rule that overrides contrary laws and regulations to establish that the legal validity of transaction documents (electronic signatures, contracts, and records) cannot be denied solely because they are in electronic form. The Act applies to all signatures, contracts, or other records "relating" to a "transaction," which is broadly defined to include "an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons." This powerful new law will overrule a wide variety of old laws and regulations that would otherwise have required contracts, signatures, or other records to be in writing or on paper.

E-SIGN is technologically neutral — it allows the parties to an agreement to determine the electronic procedures and authentication requirements they will use. For example, the Act broadly defines "electronic signature" to mean "an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." Under this definition, a wide variety of electronic actions could qualify as electronic signatures so long as they are performed with the requisite intent. Contracting parties should ensure that their computer systems have the capability of retaining the evidence necessary to prove the existence of the electronic contract or signature.

The Act states that this rule *only* affects laws that would require contracts, signatures, or records to be in *non-electronic* form. The Act also provides that the legal effect of electronic records or contracts *may* be denied if the record is not in a form that is capable of being retained and accurately reproduced for later reference by all parties who are entitled to retain the record. Finally, the Act clarifies that no person is required to use electronic contracts, signatures, or records.

The Act also expressly exempts laws regarding certain transactions, including: wills, codicils, and testamentary trusts; matters related to adoption, divorce, and family law; the UCC other than Articles 2 and 2A and sections 1-107 and 1-206; official court documents, orders, and notices, including briefs; documents required to accompany the transportation of hazardous materials;

and a variety of notices — of product recalls and hazards, of cancellations of utility service, health or life insurance, and of defaults and related actions regarding mortgages or leases on a primary residence.

- **Electronic Recordkeeping.** The Act states that legal requirements to *retain* a contract or other record (including requirements to keep "originals" and checks) may be satisfied by the use of electronic records. The e-records must accurately reflect the information set forth in the contract or record, be accessible to all who are legally entitled to access, and be in a form that can be reproduced for later reference (which can be done by printing, "transmission," or "otherwise").

- **Electronic Consumer Disclosures**. The Act also generally authorizes businesses and others to provide certain required information to consumers electronically so long as the consumer consents under the E-SIGN framework. (The Act defines a "consumer" as an individual, or their legal representative, who obtains, through a transaction, products or services which are used primarily for personal, family, or household purposes.) Specifically, the Act says that if a statute, regulation, or rule of law requires information to be provided in writing, the use of an electronic record will satisfy that requirement, if (a) the consumer is provided with detailed *pre*-consent notice of certain information and rights the consumer has, (b) the consumer affirmatively consents in a sufficiently demonstrable manner, and (c) the discloser complies with certain *post*-consent obligations to update.

    - Pre-Consent Notice. Before a consumer consents to receiving notices and records electronically, businesses must present to the consumer a "*clear and conspicuous*" statement informing them of their right to have the notices and records provided either in paper or electronically, their right to later withdraw consent and receive paper, how they may withdraw consent (and the consequences, including whether or not any fees would be charged), how they may later obtain paper copies of electronic records, and whether the consent will apply to just that particular transaction or a broader range of records. The discloser also must describe the computer equipment (hardware and software) the recipient needs to be able to access and retain the electronic disclosures.
    - Demonstrable Consent. In order to consent to the receipt of electronic transactions, the consumer must do so "affirmatively" and "in a manner that *reasonably demonstrates* that the consumer can access information in the electronic form" in which it will be disclosed.
      This may mean as a practical matter that a consumer must consent electronically in the same manner that the consumer will be receiving the e-disclosures. (For example, if the disclosures will be posted on a web site, the consumer may have to demonstrate his ability to access the disclosures by consenting on that web site.) This equirement could create a trap for the unwary, and staff for Senate Banking Chairman Phil Gramm has suggested that if this requirement is interpreted too broadly, corrective legislation could be required. Moreover, the Act requires the Commerce Department and the Federal Trade Commission specifically to study this requirement for "demonstrable consent" and report back to Congress within a year on whether its benefits to consumers outweigh its burdens on e-commerce, including whether its absence would increase the incidence of consumer fraud.
    - Post-Consent Duties. If technology changes so that there is a "material risk" that consumers will no longer be able to access or retain electronic disclosures, the discloser must provide the consumer with a statement of the new hardware or software needed, the right to withdraw consent and return to paper at no charge, and go through the entire consent procedure described above again.

What are regulators' obligations under the Act?
The Act authorizes federal and state regulators who separately have rulemaking authority under another statute (e.g., consumer disclosure statutes such as the Truth in Lending Act) to interpret how E–SIGN applies to the other statute. But the Act tightly restricts their authority: the regulators'

interpretations generally must be "consistent" with E-SIGN, supported by "substantial justification," technologically neutral, not impose unreasonable costs on the use of electronic records, and only impose requirements that are substantially equivalent to the burdens on *non*-electronic records. In case those strictures were not clear enough, the Act also specifically provides that regulators may *not* "add to" E–SIGN's requirements.

On the other hand, E-SIGN specifically authorizes regulators to set "performance standards" to assure the accuracy, integrity, and accessibility of electronic recordkeeping. In doing so, the regulators are authorized to depart from the Act's mandate for technological neutrality if such departure is "substantially related" to the achievement of "an important governmental objective" and are authorized to require paper records if "essential" to achieving a "compelling" national security or law enforcement interest. The Act also provides that it does not limit the ability of a regulatory agency to require records that are filed with the agency to be in a specified format.

Perhaps most significantly, the Act empowers federal regulators to exempt categories of transactions within their jurisdiction from the E-SIGN consent framework under certain circumstances. In this vein, the Act requires the SEC to act under this authority to issue rules by July 30 exempting registered investment companies when prospectuses, advertising, and supplemental sales literature are provided electronically. Since many regulators (e.g., the Federal Reserve Board and the SEC) have already issued guidance on electronic disclosures, there likely will be further reconciling rules.

What procedures does the Act establish for transferable records? Title II of the Act establishes procedures and requirements for the transferability of electronic promissory and mortgage notes ("transferable records") and addresses how a person may become a holder in due course under the UCC (and prove this status) by gaining control of such transferable records.

Why does the Act preempt state law? One motivation for the federal statute was the adoption by the states over the last five years of a wide variety of different electronic signature and commerce statutes. (For example, some states permit the use of any kind of electronic signature, while others require either a minimal form of security or a specific kind of digital signature technology.)

The Act provides that the states *can* modify the Act's requirements with respect to State law either by (a) adopting the Uniform Electronic Transactions Act (as approved by the National Conference on Uniform State Laws) or (b) specifying alternative procedures and requirements for electronic contracts and records that are "consistent" with E-SIGN, do not discriminate with respect to the technology involved, and, if enacted after E-SIGN, specifically refer to it.

When does the Act become effective? The law generally becomes effective October 1, 2000, with regard to electronic contracts, signatures, and consumer disclosures. The electronic recordkeeping provisions are effective on March 1, 2001, for any statutory and regulatory requirements in existence at that time, and on June 1, 2001, for any recordkeeping requirements that are part of a regulatory agency's rulemaking that has been announced but not completed by March 1, 2001.

For more information about E-SIGN, contact:

Ron Greene: 202-663-6285; rgreene@wilmer.com
David Luigs: 202-663-6451; dluigs@wilmer.com
Brandon Becker: 202-663-6979; bbecker@wilmer.com
Soo Yim: 202-663-6958; syim@wilmer.com

Monthly Update

Carnivore. On July 24, the House Judiciary Subcommittee on the Constitution held a hearing on a controversial eavesdropping program called "Carnivore" that enables the FBI to isolate, intercept and collect communications. The FBI says that many Internet service providers lack the ability to isolate the specific types of information that may be collected under a court order. One of the nation's largest ISPs, EarthLink, has refused to install Carnivore on its network because attaching the program in the past caused its remote access servers to crash, eliminating service to customers. Other ISPs have stated publicly that they would challenge any order to attach the program to their networks. Attorney General Janet Reno says she will have a group of experts conduct a

detailed review of Carnivore's source code. Those experts will report their findings to a panel of interested parties.

ENCRYPTION EXPORTS. Following the European Union's recent move to loosen export controls on encryption products, the Clinton Administration announced on July 17 that it would eliminate the distinction between retail and non-retail products, as well as the restrictions on government end-users for some countries. The new rules, which could take effect next month, will allow exporters to sell more easily their products to the European Union's 15 member countries and Japan, Australia, New Zealand, Poland, the Czech Republic, Hungary, Norway, and Switzerland. The plan also removes a previously-required 30-day technical review, allowing companies to ship their products immediately.

INTERNET GAMBLING. Although the Senate easily passed the Internet Gambling Prohibition Act of 1999 (S. 692) last year, the House version, H.R. 3125, has not fared so well. The legislation was considered in the House under an expedited procedure, usually reserved for non-controversial bills, which requires a supermajority vote to pass. While achieving a significant majority, the bill did not receive the necessary two-thirds vote. House leaders must now consider whether or not to bring up the bill under a rule which would set the terms of debate and provide for amendments. The legislation faces bipartisan opposition, including some who oppose any regulation of the Internet and others who believe the bill does not go far enough to stop illegal gambling. The bill makes it unlawful for a person engaged in a gambling business to use the Internet or any other interactive computer service to place, receive, or otherwise make a bet or wager; or to send, receive, or invite information assisting in the placing of a bet or wager.

NAPSTER. On July 26, federal district court judge Marilyn Hall Patel (N.D.Ca.) ordered Napster to shut down the portion of its site that allows people to exchange copyrighted MP3 music files. Napster is being sued by several major record companies for copyright infringement. Napster had argued that it should be protected from liability under the safe harbor provisions of the Digital Millennium Copyright Act of 1998 (DMCA), and that its technology was capable of substantial noninfringing uses. Napster has obtained a stay of Judge Patel's order from the Ninth Circuit.

PRIVACY: FEDERAL LEGISLATION. On July 26, Senator John McCain (R-AZ), Chairman of the Senate Commerce Science and Transportation Committee, introduced The Consumer Internet Privacy Enhancement Act (S. 2928). The bill is cosponsored by Senators John Kerry (D-MA), Spencer Abraham (R-MI), and Barbara Boxer (D-CA). The legislation would require web site operators to post notice of their practices with respect to the collection of personally identifiable information. Consumers would have the right to limit the sharing of their personal information with third parties for purposes unrelated to the products and services provided by the web site that collected the information. Penalties would be $22,000 a day, up to $500,000, and the Federal Trade Commission would have enforcement power. State attorneys general also could bring suits in federal court under the Act. The bill would preempt state law to ensure that the law governing the collection of personally identifiable information is uniform. Additionally, the bill would direct the National Academy of Sciences to examine the collection of personal information in the offline world as well as methods to provide consumers with access to information collected about them.

PRIVACY: SAFE HARBOR. On July 27, the European Commission provided its formal opinion that the "safe harbor" agreement that had been negotiated between the U.S. and the EU provides "adequate" protection for EU personal data. See *http//:www.ita.doc.gov/ecom*. The EU bans the flow of personal data from Europe to countries that are deemed to have inadequate privacy protections. The agreement will go into effect in 90 days and will be reevaluated next year. U.S. companies must commit to detailed privacy principles, such as access and notice, in order to gain protection under the agreement. The Federal Trade Commission can take action against a company if it promises to abide by the principles but fails to do so.

SPAM. On July 18, the House passed the Unsolicited Commercial Electronic Mail Act of 2000 (H.R. 3113), sponsored by Reps. Heather Wilson (R-NM) and Gene Green (D-TX) by an

overwhelming vote of 427-1. The legislation would require unsolicited, commercial e-mail to include a header identifying the message as an advertisement and to have a valid return e-mail address that recipients may use to request that they be removed from the distribution list. It would be illegal to continue sending such e-mail. On May 11, Sen. Conrad Burns (R-MT) introduced similar legislation (S. 2542) in the Senate. A spokesman for Sen. Burns says the Senate Commerce Science and Transportation Committee may bypass hearings on the bill and move straight to a markup and vote. The spokesman said that "spamming has been almost hearing-ed out. The feeling is that most members have enough knowledge of this issue by this point in time that a hearing may not be necessary." However, there are only five weeks remaining in the session following Congress's return from its August recess after Labor Day.

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.

ECommerce News is a publication of WCP's EGroup.