VEDDER PRICE
VEDDER, PRICE, KAUFMAN & KAMMHOLZ, P.C.

May, 2005

Electronic and Computer Generated Records

By Timothy J. Carroll

I. INTRODUCTION

Electronic records can be divided into two groups:

(1) those generated electronically for which no paper original exists — *e.g.*, e-mail, electronic invoices, records of electronic data interchange, etc; and

(2) those which were originally on paper but have been transferred to some form of electronic storage — *e.g.*, microfilm, magnetic tape, etc.

A. Advantages of Electronic Records

1. Reduced Storage Space

The most significant advantage to electronic records, over traditional paper records, is the reduction in the space required for storage. Instead of rooms full of filing cabinets, the records may require only a drawer full of computer disks. The reduction in space also results in reduced storage costs.

2. Faster Search and Retrieval

Another major advantage of electronic records is the ability to conduct a computerized search for a particular record rather than to leaf manually through stacks of paper documents. Even the most organized and best maintained paper system is likely to result in misfiled or lost information.

3. Ease of Reproduction

Not only are electronic records easier to locate, they are easier to copy. It may even be reasonable to make duplicate copies and store them off-site in case the originals are lost or destroyed.

4. Original Data in Electronic Form

As a result of the increased use of electronic data interchange, many transactions occur solely in the electronic universe. Rather than generating paper records for these transactions, companies may want simply to retain the electronic records. In fact, the IRS may require that these records be maintained in their original format.

B. Disadvantages of Electronic Records

1. Backup Records

One of the greatest disadvantages of electronic records is their vulnerability to loss. Changes in temperature or humidity can damage computer systems and magnetic tape. Likewise, these mediums have only a certain "shelflife" and they must be replaced on a regular basis. Thus, any electronic records retention policy will require a routine process for creating accurate backups and ensuring integrity of existing records.

2. Preventing Alteration

It may also be difficult to detect alterations made to electronic records. There will not be neatly penned notes in the margin or entire sections crossed out. Thus, to prevent unauthorized alteration, the company will need to establish security measures and access requirements to limit the ability of employees and other agents to make unauthorized alterations.

3. Storage

Storing disks or magnetic tape containing the records in a desk drawer is not an acceptable practice. The records must be stored in a controlled environment to prevent damage. Often, this means either building the proper facility on site, with the requisite environmental controls, or contracting with a third party to properly store the records.

4. Paper Requirements

In some situations, a company using computerized records may also be required to maintain paper records of the same transaction, particularly under the IRS regulations.

5. System Changes

When the company adopts a new computer/record system, it will generally be required to transfer all of its existing documents to that system. While this may not be difficult in some situations, it could prove not only difficult but very expensive when the new and old systems are not compatible. The same issues may be faced in the merger or the acquisition of another company which uses a different system.

6. Evaluation Before Creation

Paper records can be created, stored, and reviewed many years later. While the same is technically true for electronic records, often these records will be lost before their value can be determined, especially in the case of records created by employees, such as word processing documents and e-mail. To prevent that

problem, it may be necessary to designate during the creation stage whether documents will need to be retained (either electronically or in paper format).

II. Electronic Records and Federal Compliance

A variety of federal agencies require corporations to maintain records on specific topics and in a specific manner. Most permit the storing of records in an electronic format so long as they can be accessed upon demand. *See, e.g.*, 21 C.F.R. § 211.180 (FDA regulations for batch drugs: "Records that can be immediately retrieved from another location by computer or other electronic means shall be considered as meeting the requirements of this paragraph."); 10 C.F.R. § 34.87 (Department of Energy Regulations: "The records may also be stored in electronic media with the capability for producing legible, accurate, and complete records during the required retention period.").

A. IRS Regulations

The IRS has the most complete and helpful regulations relating to electronic records. The Internal Revenue Code is built around a "voluntary" system of payment — that is, each taxpayer determines its own tax liability. The IRS checks only a small percentage of returns for accuracy. Once audited, however, the taxpayer has the burden to document all income and justify any deductions. Title 26 C.F.R. § 1.6001-1(a) requires each taxpayer to maintain and produce records relating to its return. Failure to produce the required documentation most often results in a denial of the deduction and, therefore, an increase in tax liability. Stronger penalties may be assessed if the error resulted from negligence or intentional wrongdoing on the part of the taxpayer. While taxpayers may employ third parties to process and/or store their records, it does not relieve the taxpayer of the duty to produce records.

Not every record produced by the taxpayer must be retained. Section 1.6001-1(e) requires that the records be maintained and made available to IRS inspection, but only for as long as the records may be material in the administration of any Internal Revenue law. Some records are never material. For example, a letter requesting information about a product that did not lead to a sale is unlikely to have any effect on Internal Revenue law and would not have to be maintained for IRS purposes. Note, however, that this letter might be material for other purposes, *e.g.*, in an allegation of misrepresentation. Other records may be material when created, but may lose that character over time. This might include records relating to past tax liability in a year for which the statute of limitations has passed, thus preventing the IRS from challenging the return. Other records may be material when created and retain that character permanently or long after the statute of limitations expires. For example, documents relating to the purchase of a building whose value has depreciated over a long period of time would be material to tax years even after the statute expired for the year of purchase.

Treasury Regulation § 31.6001-1(e) requires that records be retained for at least four years after the date of filing for the return to which they relate or the date on which the tax is paid, whichever is later. As noted above, however, records must be maintained for as long as they are or might be relevant to Internal Revenue law, even if that period extends beyond four years. As a general rule, the period of materiality can be measured by the statute of limitations relating to the tax return. In the normal case, a return may be audited only within three years of its filing date. *See* IRC § 6501. After that time, most records are no longer "material." In certain circumstances, however, the period for audit may be extended. For example, if amounts were omitted from gross income and those amounts exceed 25 percent of the income reported, the return is subject to audit for six

years after its filing date. If the IRS alleges a fraudulent return or willful tax evasion, it may audit the return at any time — there is no statute of limitations in that circumstance. If conduct may have occurred that might permit the IRS to extend the deadline for audit, records should be maintained for longer than the required four years. Also, remember that some records may have materiality far in excess of any applicable statute of limitations period.

In addition to the foregoing rules relating to general business records, the IRS has developed specific rules for both types of electronic records — those generated by computer and those transferred to electronic/nonpaper format.

1. Revenue Procedure 98-25 — Automatic Data Processing Systems

Revenue Procedure 98-25 (Rev. Proc. 98-25) updates and supercedes Revenue Procedure 91-59, which formerly governed the use of electronic records for tax purposes. The new procedure applies for taxable years beginning after December 31, 1997. Rev. Proc. 98-25 permits a taxpayer to retain records in a machine-sensible format, defined as "data used in an electronic format that is intended for use by a computer." It does not include paper records or paper records that have been converted to an electronic storage medium, *e.g.*, microfiche. Records maintained under Rev. Proc. 98-25 must be capable of being processed, defined as "the ability to retrieve, manipulate, print on paper (hard copy), and produce output on electronic media."

Revenue Procedure 98-25 applies to all taxpayers with "assets of $10 million or more at the end of the taxable year." Taxpayers with fewer assets, however, are not immune. They must follow Rev. Proc. 98-25 if they use machine-sensible records and do not maintain paper records, or if the machine-sensible records were used for computations that cannot be verified without use of a computer, *e.g.*, complicated last-in first-out (LIFO) inventories. The same statute of limitations and materiality issues discussed above for paper records also apply to electronic records.

Compliance with Rev. Proc. 98-25 requires the taxpayer to demonstrate that its electronic records procedure "provide[s] sufficient information to support and verify entries made on the taxpayer's return and to determine the correct tax liability." Generally, this means demonstrating an audit trail between the records and the total amount of tax liability claimed. However, a taxpayer that does not generate machine-sensible records in the ordinary course of its business is not required to produce them for the IRS. If the records retained do not contain all of the necessary data to identify the transaction, the taxpayer is required to supplement those records with hard copy records.

The taxpayer is also required to document the process that created the documents. Documentation is required for any business processes that

(1) create the retained records;

(2) modify and maintain the records;

(3) satisfy the requirement of § 5.01(2) of this revenue procedure [relating to database management systems] to support and verify entries made on the taxpayer's return and determine the correct tax liability; and

(4) evidence the authenticity and integrity of the taxpayer's records.

Documentation will be sufficient if it describes the function performed and the internal controls that ensure accuracy and prevent unauthorized alterations, and provides detailed account descriptions. In addition, for each file maintained, the taxpayer must document the record format, field definitions, file descriptions, periodic checks to satisfy maintenance requirements, reconciliation between the records and the taxpayer's books, and reconciliation between the records and the tax return filed.

All of the above records and documentation must be provided to the IRS upon request. If the files require special resources for access, *e.g.*, a special program on the taxpayer's computer system, the taxpayer is required to provide those resources. Access must be granted without limitation such as by a contract or license. The taxpayer may, however, be able to reach an agreement with the IRS, whereby the files can be converted to another system or accessed during off-peak hours. Further, the taxpayer may provide the IRS with third-party equipment in order to access the files.

If records become unavailable for any reason, the taxpayer is required to notify the IRS immediately. This includes records that are lost, stolen, destroyed, damaged, otherwise incapable of being processed, or are found to be incomplete or materially inaccurate. As part of the notice, the taxpayer needs to identify the records that were lost and suggest a plan for how and when the taxpayer will replace the records. In some situations, the IRS may be willing to permit only partial restoration of the missing data.

Revenue Procedure 98-25 also makes the following recommendations for maintenance of electronic records:

(1) proper labeling;
(2) secure storage environment;
(3) creating backup copies;
(4) selecting an off-site storage facility; and
(5) testing to confirm records integrity.

The IRS also suggests that taxpayers consult the National Archives and Records Administration's (NARA) Standards for the creation, use, preservation, and disposition of electronic records, 36 C.F.R. § 1234. In fact, the IRS will not impose penalties for partial loss of data if the NARA standards were followed. The taxpayer will, however, still have to substantiate the tax liability claimed on the return.

As noted above, compliance with Rev. Proc. 98-25 does not relieve taxpayers of the duty to retain hard copy records generated in the ordinary course of their business. Hard copies may, however, be maintained on microfiche/microfilm (in compliance with Rev. Proc. 81-46) or in an electronic storage system (in compliance with Rev. Proc. 97-22, discussed below). The taxpayer is not required to generate paper records if they are simply computer printouts, not produced in the ordinary course of business, or if all the details of the transaction are maintained in machine-sensible records conforming to this revenue procedure. The taxpayer may, however, be requested to generate a hard copy as part of an IRS audit.

2. Revenue Procedure 97-22 — Electronic Storage Systems

Revenue Procedure 97-22 outlines the procedure by which taxpayers may convert hard copy records to an electronic storage system (ESS). An ESS is a system to prepare, record, transfer, index, store, preserve, retrieve, and reproduce books and records by either:

(1) electronically imaging hard copy documents to electronic storage media; or

(2) transferring computerized books and records to electronic storage media using a technique such as "COLD" (computer output to laser disk), which allows books and records to be viewed or reproduced without the original program.

For any ESS maintained, the taxpayer must be able to provide a complete description of the system and the procedures related to its use as well as the indexing system.

In general, an ESS will be acceptable so long as it includes the following:

- reasonable controls to ensure the integrity, accuracy, and reliability of the system;
- reasonable controls to prevent and detect the unauthorized creation of, addition to, alteration of, deletion of, or deterioration of electronically stored records;
- an inspection and quality assurance program evidenced by regular evaluations of the electronic storage system including periodic checks of electronically stored books and records;
- a retrieval system that includes an indexing system; and
- the ability to reproduce legible and readable hard copies.

The ESS may be subject to periodic testing by the IRS. The test may include "an evaluation (by actual testing) of a taxpayer's equipment and software, as well as the procedures used by a taxpayer to prepare, record, transfer, index, store, preserve, retrieve, and reproduce electronically stored documents." If the IRS chooses to make a test, the taxpayer is required to retrieve and produce the requested documents (including hard copies if requested) and to provide the IRS with the resources necessary to locate, retrieve, read, and reproduce the records. For this reason, it is again necessary that neither the hardware nor software be subject to any contract or license restriction that would prevent access by the IRS.

As with Rev. Proc. 98-25, records kept in ESS must be retained as long as they might be material. Further, the use of a third party for storage does not relieve the taxpayer of the duty to produce the records. The IRS also recommends maintaining ESS in the same way as electronic records, *i.e.*, labeling, off-site storage, etc. Again, however, it recognizes that these procedures are business decisions best left to the individual taxpayer.

Original hard copy documents, other than machine—sensible documents subject to Rev. Proc. 98-25, may be destroyed after the taxpayer has

(1) completed its own testing of the ESS that established that hard copies or computerized books and records are being reproduced in compliance with all provisions of this revenue procedure; and

(2) instituted procedures that ensure compliance with all the provisions of this revenue procedure.

3. Records Evaluations and Record Retention Limitation Agreements

Revenue Procedure 98-25 provides the opportunity for the taxpayer to seek a records retention evaluation by the IRS. Either at the request of the taxpayer or upon its own initiative, the IRS may "review the taxpayer's record retention practices, including the taxpayer's relevant data processing and accounting systems." Further, the IRS "may periodically initiate tests to establish the authenticity, readability, completeness, and integrity of a taxpayer's machine-sensible records retained in conformity with this revenue procedure." A records evaluation is not an "examination," "investigation," or "inspection" within the meaning of § 7605 because it is not directly related to a determination of tax liability. A records evaluation may be desirable for your company because it will allow you to identify problems and correct them before they cause or enhance tax deficiencies.

The taxpayer also may enter into a Record Retention Limitation Agreement (RRLA) with the IRS. As part of the request, the taxpayer must "identify and describe those records the taxpayer proposes not to retain and explain why those records will not become material to the administration of any Internal Revenue law." In response to the request, the IRS may waive any or all of the requirements of Rev. Proc. 98-25. The RRLA will not, however, apply to any system added after the RRLA was issued. The taxpayer will need to seek a new RRLA for that system. Likewise, the RRLA generally does not apply to subsidiaries acquired after the RRLA was issued. Further, if a subsidiary is sold, the parent must continue to retain any documents under the RRLA until a new ruling is issued. An RRLA does not relieve the taxpayer of records retention requirements or of the duties under § 6001. It simply provides greater freedom in determining how those requirements are met.

B. Indexing and Retrieval

Generally, a company is free to maintain its records in any manner it chooses as long as those records can be retrieved in a reasonable and legible manner when requested. For electronic records, this means that the company could simply download files to a mainframe without any type of organization. Some federal regulation, however, may require that documents be maintained or indexed in a particular fashion. The following list includes some of the other federal regulations specifying a manner of organization, maintenance, or indexing:

- The U.S. Department of Energy requires manufacturers to maintain an index of records relating to certification tests for energy conservation. *See* 10 C.F.R. § 430.62.
- The Federal Aviation Administration requires an index for air carrier records maintained in a machine-readable format. *See* 14 C.F.R. §§ 249.3, 249.4, and 249.20.
- The Bureau of Export Management requires an index of all records for transactions involving restrictive trade practices or boycotts, exports of technology, exports to Canada, etc. *See* 15 C.F.R. part 762.
- The Food and Drug Administration requires an index for all electronic records of manufactures related to medical devices. *See* 21 C.F.R. § 814.82.
- The Environmental Protection Agency requires automobile manufacturers to maintain records with an index of emission certification records. *See* 40 C.F.R. § 86.091-7.

Even if a particular indexing method is not required, the corporation is still responsible for producing the records during an audit by a regulatory agency. If the records are maintained in a fashion that prevents retrieval, they will be considered destroyed even if they do in fact exist. This is considered *de facto* destruction.

If they are required to produce documents under a subpoena or discovery request, corporations may also run into trouble due to poor organization or indexing. The Federal Rules of Civil Procedure now requires parties in litigation to turn over relevant documents early in the case, even if not requested by the other side.

III. Myths about Electronic Records

A. Gone but Not Forgotten

By far the most common myth regarding computers and computer data relates to the delete function. Many people wrongly assume the delete key removes data from the hard drive. When the computer is told to "delete" a file, however, it simply removes the file's name from the directory and designates that space on the hard drive as available. The file is not actually removed until the computer determines that no unused space is available to write other files. At that point, a new file may be written over the old file, and it will be gone forever. Even then, however, the computer uses existing space in a random manner. Thus, depending on the size of a hard drive, "deleted" files could remain on the computer indefinitely. Depending on the type of system used, this may also be true for e-mail and voice mail communications.

Files that were deleted but not really removed can be the subject of a discovery request. In fact, because there most likely was a reason for deleting the files in the first place, they are often some of the first records sought.

A company has several options to prevent discovery of deleted files. The first is to simply prevent the file from being generated in the first place. In many cases, the best tactic is to simply walk down the hall to a co-worker's office and discuss a subject orally. A second option is to purchase software designed to remove deleted files from a computer. These programs simply place a series of ones anywhere on the disk designated as available. If this option is selected, however, it is important to make use of the software part of the records destruction routine. A final option is to hire a company specializing in the destruction of computer records.

B. The Information behind the Screen

A second myth about electronic data is that a printout is an exact copy of the file. While a printout may be an exact copy of the words on the screen, and will often be admitted into evidence as such, it does not reveal the other information gathered and stored by the computer program. For example, many word-processing programs routinely create a "log file" or "audit trail" with a record of the date and time stamp and who originated the document. Other programs automatically save files to the hard drive at regular intervals. Thus, it may be possible for a copy to exist on the disk even if the user never pressed the save key. E-mail messages also include a lot of information beyond the intended message, including who sent the message, where it was sent, the date of the transmission, if it was forwarded, etc. An adversary could access this information to determine when files were created or modified, often providing invaluable information.

IV. Special Problems Related to E-mail

E-mail has become one of the most valuable tools for business; it allows quick and efficient transmission of information throughout an organization and beyond. It has also become the "smoking-gun" of litigation in the 1990s.

Not only do many users treat e-mail too informally, they also continue to treat it as though it is private. The reality is, however, that e-mail is not private. Once a message leaves an employee's computer, the employee loses control of the e-mail. Servers often route the message through various networks and possibly over the Internet before it reaches its final destination, providing ample opportunity for competitors to obtain what could be confidential information about the company.

A second problem with e-mail is that it may be unexpectedly recorded by the employee's computer, the receiver's computer, or by any computer through which it passes. Even if the company has an excellent records retention and destruction program in place to erase unnecessary e-mail, it cannot control whether others retain e-mail after it has been designated for destruction. If a copy is available from any of these sources, it could be introduced against the company in litigation. Indeed, e-mail typically is admissible as a business record under federal and state rules of evidence.

Therefore, special precautions should be taken with respect to e-mail, including the following:

- Instruct employees on the proper uses of e-mail. They should treat it as any other business correspondence, i.e., use proper grammar, check for spelling, avoid insulting remarks, etc. They should also recognize that it may be read by many people other than the intended recipient.

- Segregate e-mail messages when making backup copies of the computer system. They should be deleted in a short time, usually fifteen to thirty days, and this can only be accomplished if they are located in a separate backup file. Segregating may also make searching for particular messages easier when complying with a discovery request.

- Establish a procedure for determining when e-mail should be kept longer than the allotted time. If e-mail is important enough to be retained, the company probably needs to establish a way to convert it to a formal business record. Note, however, that simply printing the e-mail is not sufficient, as this does not retain information about its origination, destination, date of creation, etc.

- Instruct employees not to use e-mail for confidential or privileged communications. Because of the danger of third-party interception, the expectation of privacy may not be justified and the privilege may be lost.

V. ELECTRONIC RECORDS RETENTION UNDER UETA AND THE E-SIGN ACT

Two recent laws establish retention requirements for electronic records. The first is the Uniform Electronic Transactions Act (UETA), which was approved in July 1999 by the National Conference of Commissioners on Uniform State Laws, and has since been adopted in several states. The second is the Electronic Signatures in Global and National Commerce Act, also known as the E-SIGN Act, which was signed by President Clinton on June 30, 2000.

A. UETA

1. Scope

Basically, UETA is a procedural, as opposed to a substantive, statute that applies to electronic records and electronic signatures relating to a transaction. A "transaction" is "an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs." *See* § 2(16). An electronic signature is defined in § 2(8) as "an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record." A "signature" includes standard Web page click-through agreements and also applies to the inclusion of a name on an e-mail message. The requirement that the signature be "attached to or logically associated with a record" was added in recognition that, unlike a paper record, the electronic signature will not be physically attached to the electronic record. Therefore, it is important to demonstrate in some other way that the signature refers to a particular record.

An electronic record is defined in § 2(7) as "a record created, generated, sent, communicated, received, or stored by electronic means." According to the Official Comments, an electronic record applies to information "stored on a computer hard drive or floppy disc, facsimiles, voice mail messages, messages on a telephone answering machine, [and] audio and video tape recordings . . . ."

2. Legal Recognition of Electronic Records and Signatures

Section 7, "Legal Recognition of Electronic Records, Electronic Signatures, and Electronic Contracts," states that a record or signature cannot be denied legal effect merely because it is in electronic form, and that an electronic record satisfies a requirement that a record be in writing. This section also states that an electronic signature satisfies a signature requirement, and that a contract cannot be denied legal effect if an electronic record was used in its formation.

Note that this section does not state that electronic signatures and records will be given effect or be enforceable. Those determinations are left to other legal requirements.

3. Record Retention Requirements — Generally

UETA also explicitly provides for the use of electronic records in record-keeping procedures. Section 12, "Retention of Electronic Records; Originals," provides as follows:

(a) If a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record which:

(1) accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise; and

(2) remains accessible for later reference.

(b) A requirement to retain a record in accordance with subsection (a) does not apply to any information, the sole purpose of which is to enable the record to be sent, communicated, or received.

(c) A person may satisfy subsection (a) by using the services of another person if the requirements of that subsection are satisfied.

(d) If a law requires a record to be presented or retained in its original form, or provides consequences if the record is not presented or retained in its original form, that law is satisfied by an electronic record retained in accordance with subsection (a).

(e) If a law requires retention of a check, that requirement is satisfied by retention of an electronic record of the information on the front and back of the check, in accordance with subsection (a).

(f) A record retained as an electronic record, in accordance with subsection (a), satisfies a law requiring a person to retain a record for evidentiary, audit, or like purposes, unless a law enacted after the effective date of this [Act] specifically prohibits the use of an electronic record for the specified purpose.

(g) This section does not preclude a governmental agency of this state from specifying additional requirements for the retention of a record, subject to the agency's jurisdiction.

According to the Comments, this section is concerned with maintaining the integrity of the information in the record, as opposed to retaining the "original" record. The Comments note that, owing to the way information on a computer is saved or stored, it could be argued that the "original" of a record can be easily destroyed. Thus, this section concentrates on ensuring that the record's information is accurate. See § 12, cmt. 2.

Further, the Comments emphasize the importance of updating the technology used to store an electronic record. For an electronic record to be valid, it must be accessible. Thus, the technology originally used to store the record must be updated to be compatible with the emerging technology. *See* § 12, cmt. 3. Lastly, once a written record is stored electronically, the original written record can be destroyed. *Id.*

In addition, under § 13, "Admissibility in Evidence," electronic records can be admitted as evidence. "In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form."

4. Record Retention Requirements — State Governments

Sections 17 through 19 are optional provisions that address procedures for state governments to retain electronic records. While a state does not have to adopt these sections, if a state is acting as a commercial party, UETA will apply, according to the Comments. This means that the state government "must agree to conduct transactions electronically with vendors and customers of government services" *See* § 19, cmt. 1.

SECTION 17. CREATION AND RETENTION OF ELECTRONIC RECORDS AND CONVERSION OF WRITTEN RECORDS BY GOVERNMENTAL AGENCIES. [Each governmental agency] [The [designated state officer]] of this state shall determine whether, and the extent to which, [it] [a governmental agency] will create and retain electronic records and convert written records to electronic records.

SECTION 18. ACCEPTANCE AND DISTRIBUTION OF ELECTRONIC RECORDS BY GOVERNMENTAL AGENCIES.

(a) Except as otherwise provided in § 12(f), [each governmental agency] [the [designated state officer]] of this state shall determine whether, and the extent to which, [it] [a governmental agency] will send and accept electronic records and electronic signatures to and from other persons and otherwise create, generate, communicate, store, process, use, and rely upon electronic records and electronic signatures.

(b) To the extent that a governmental agency uses electronic records and electronic signatures under subsection (a), the [governmental agency] [designated state officer], giving due consideration to security, may specify:

(1) the manner and format in which the electronic records must be created, generated, sent, communicated, received, and stored and the systems established for those purposes;

(2) if electronic records must be signed by electronic means, the type of electronic signature required, the manner and format in which the electronic signature must be affixed to the electronic record, and the identity of, or criteria that must be met by, any third party used by a person filing a document to facilitate the process;

(3) control processes and procedures as appropriate to ensure adequate preservation, disposition, integrity, security, confidentiality, and auditability of electronic records; and

(4) any other required attributes for electronic records which are specified for corresponding nonelectronic records or reasonably necessary under the circumstances.

(c) Except as otherwise provided in § 12(f), this [Act] does not require a governmental agency of this state to use or permit the use of electronic records or electronic signatures.

SECTION 19. INTEROPERABILITY. The [governmental agency] [designated officer] of this state which adopts standards pursuant to § 18 may encourage and promote consistency and interoperability with similar requirements adopted by other governmental agencies of this and other states and the federal government and nongovernmental persons interacting with governmental agencies of this state. If appropriate, those standards may specify differing levels of standards from which governmental agencies of this state may choose in implementing the most appropriate standard for a particular application.

5. Notice and Writing Requirements

Many laws require that certain parties receive written notification of certain events. Section 8, "Provision of Information in Writing; Presentation of Records," allows such notice to be provided electronically. The Comments indicate that this section is a "savings provision," designed to prevent the Act from overriding other aspects of a "writing" required by other law. In order to satisfy this section, the recipient of the electronic record must not only be able to read it, but must also be able to either print it out or store it for future reference. If the sender's computer or communication device prevents either of those actions, the writing will not satisfy this requirement. The section also makes clear that laws regarding the means of delivery are not affected by the

Act. However, a law requiring delivery by first-class mail would be satisfied even if the information was sent in electronic format on a disk.

6. Attribution

Because an electronic signature, particularly a click-through Web agreement, is often done anonymously, it is important for the parties to have some way of attributing that "signature" to a particular party. Section 9, "Attribution and Effect of Electronic Record and Electronic Signature," governs how attribution will be handled. It states:

> (a) An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to whom the electronic record or electronic signature was attributable.
>
> (b) The effect of an electronic record or electronic signature attributed to a person under subsection (a) is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement, if any, and otherwise as provided by law.

Compliance with an established security procedure is some evidence, but not conclusive evidence, that a particular electronic signature should be attributed to a particular individual. The use of security/attribution procedures is particularly important if an agreement is a click-through transaction. In that case, the security/attribution procedure may be the only way of identifying the person to whom the signature is to be attributed.

B. E-SIGN Act

1. Title I — Electronic Records and Signatures in Commerce

Title I generally gives validity to instruments of electronic commerce. Section 101 prohibits any law, other than the E-SIGN Act, from denying the legal effect of electronic signatures or contracts formed using electronic records or signatures. The legal effect of an instrument can also not be denied if it was formed by electronic agents, as long as "the action of any such electronic agent is legally attributable to the person to be bound." § 101(h).

Under § 102, the E-SIGN Act preempts state law to provide a uniform system concerning electronic records and signatures, until the states adopt UETA or other standards consistent with UETA. At such time, the federal preemption will be lifted.

In addition, § 103 also allows for exceptions to § 101. Specifically, § 103 states that § 101 will not apply to a contract or record governed by:

> (1) a statute, regulation, or other rule of law governing the creation and execution of wills, codicils, or testamentary trusts;

(2) a state statute, regulation, or other rule of law governing adoption, divorce, or other matters of family law; or

(3) the Uniform Commercial Code, as in effect in any state, other than §§ 1-107 and 1-206 and Articles 2 and 2A.

Section 101 will also not apply to court notices, orders, or official documents; notices of termination of utilities; notices of default, acceleration, foreclosure, repossession, eviction, or right to cure; notice of cancellation of health or life insurance; notice of recall of a product; and documents required to accompany the transportation of hazardous materials.

While the E-SIGN Act allows for the use of electronic records and signatures, § 101 does not require parties to use electronic records or signatures and does not limit or affect other requirements with regard to contracts imposed by law.

a. Consumer Consent

Under § 101, if certain information is required to be submitted to a consumer in writing, use of an electronic record can be used, as long as the consumer affirmatively consents to the use of an electronic record and is provided full disclosure of his or her rights and/or obligations. For example, the consumer must be informed that she or he has the right to require a written record and, following certain procedures, can withdraw her or his consent. Further, a recording of any oral communications made by the consumer is not considered an electronic record under this Act.

b. Record Retention Requirements — Generally

Section 101 sets forth the requirements for retention of contracts and records.

(1) ACCURACY AND ACCESSIBILITY — If a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be retained, that requirement is met by retaining an electronic record of the information in the contract or other record that —

(A) accurately reflects the information set forth in the contract or other record; and

(B) remains accessible to all persons who are entitled to access by statute, regulation, or rule of law, for the period required by such statute, regulation, or rule of law, in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise.

(2) EXCEPTION — A requirement to retain a contract or other record in accordance with ¶ (1) does not apply to any information whose sole purpose is to enable the contract or other record to be sent, communicated, or received.

(3) ORIGINALS — If a statute, regulation, or other rule of law requires a contract or other record relating to a transaction in or affecting interstate or foreign commerce to be provided, available, or

retained in its original form, or provides consequences if the contract or other record is not provided, available, or retained in its original form, that statute, regulation, or rule of law is satisfied by an electronic record that complies with ¶ (1).

(4) CHECKS — If a statute, regulation, or other rule of law requires the retention of a check, that requirement is satisfied by retention of an electronic record of the information on the front and back of the check in accordance with ¶(1).

A record, required to be in writing, can be denied legal effect in electronic form if it is incapable of being retained or reproduced later. § 101(e). For records that must be notarized, a notary must attach or associate her or his electronic signature, including all other required information, to the subject electronic record or signature. § 101(g).

c. Record Retention Requirements — Federal and State Governments

Section 104 addresses the applicability of Title I to federal and state regulatory agencies. Basically, this section allows regulatory agencies to issue regulations or guidance interpreting § 101, with some limitations, in conjunction with other statutes that allow such issuance. Further, this section permits federal or state regulatory authorities to require retention of tangible records, as opposed to electronic records, only if there is a "compelling governmental interest relating to law enforcement or national security." § 104(b)(3)(B). Federal agencies can also exempt a specific type of record from the consent requirements under § 101(c), under certain conditions.

The following is part of § 104.

(3) PERFORMANCE STANDARDS —

(A) ACCURACY, RECORD INTEGRITY, ACCESSIBILITY — Notwithstanding ¶ (2)(C)(iii), a federal regulatory agency or state regulatory agency may interpret § 101(d) to specify performance standards to assure accuracy, record integrity, and accessibility of records that are required to be retained. Such performance standards may be specified in a manner that imposes a requirement in violation of ¶ (2)(C)(iii) if the requirement (i) serves an important governmental objective; and (ii) is substantially related to the achievement of that objective. Nothing in this paragraph shall be construed to grant any federal regulatory agency or state regulatory agency authority to require use of a particular type of software or hardware in order to comply with § 101(d).

(B) PAPER OR PRINTED FORM — Notwithstanding subsection (c)(1), a federal regulatory agency or state regulatory agency may interpret § 101(d) to require retention of a record in a tangible printed or paper form if —

(i) there is a compelling governmental interest relating to law enforcement or national security for imposing such requirement; and

(ii) imposing such requirement is essential to attaining such interest.

(4) EXCEPTIONS FOR ACTIONS BY GOVERNMENT AS MARKET PARTICIPANT — Paragraph (2)(C)(iii) shall not apply to the statutes, regulations, or other rules of law governing procurement by the federal or any state government, or any agency or instrumentality thereof.

(c) ADDITIONAL LIMITATIONS —

(1) REIMPOSING PAPER PROHIBITED — Nothing in subsection (b) (other than ¶ (3) (B) thereof) shall be construed to grant any federal regulatory agency or state regulatory agency authority to impose or reimpose any requirement that a record be in a tangible printed or paper form.

(2) CONTINUING OBLIGATION UNDER GOVERNMENT PAPERWORK ELIMINATION ACT — Nothing in subsection (a) or (b) relieves any federal regulatory agency of its obligations under the Government Paperwork Elimination Act (title XVII of Public Law No. 105-277).

(d) AUTHORITY TO EXEMPT FROM CONSENT PROVISION —

(1) IN GENERAL — A federal regulatory agency may, with respect to matter within its jurisdiction, by regulation or order issued after notice and an opportunity for public comment, exempt without condition a specified category or type of record from the requirements relating to consent in § 101(c) if such exemption is necessary to eliminate a substantial burden on electronic commerce and will not increase the material risk of harm to consumers.

(2) PROSPECTUSES — Within thirty days after the date of enactment of this Act, the Securities and Exchange Commission shall issue a regulation or order pursuant to ¶ (1) exempting from § 101(c) any records that are required to be provided in order to allow advertising, sales literature, or other information concerning a security issued by an investment company that is registered under the Investment Company Act of 1940, or concerning the issuer thereof, to be excluded from the definition of a prospectus under § 2(a)(10)(A) of the Securities Act of 1933.

Subsection (e) provides that the Federal Communications Commission must recognize a "contract for telecommunications or letter of agency for a preferred carrier change," even though it was formed using an electronic record or signature.

d. Terminology and Scope

Under the E-SIGN Act, such terms as "electronic agent," "electronic record," and "electronic signature" are defined almost identically as they are in UETA. However, the term "transaction" in the E-SIGN Act is intentionally narrower than in UETA, in that it refers solely to commercial use. *See* S.R. 106-131.

e. Effective Dates

Title I went into effect on October 1, 2000. However, if a record retention requirement is imposed by federal or state law, then the requirements of Title I do not go into effect until March l, 2001. With regard to guaranteed and insured loans, Title I only applies to such loans made on or after one year after the date of Title

I's enactment. Finally, Title I does not apply to federal student loans until either October 1, 2001, or until the Secretary of Education publishes new promissory notes, whichever is earlier. § 107.

2. Title II — Transferable Records

Under Title II, a transferable record means an electronic record considered to be a note under UCC Article 3, and relates to a loan secured by real property. Further, the issuer of the electronic record must agree that the electronic record is a transferable record. Control of a transferable record is determined by whether the "system employed for evidencing the transfer of interests in the transferable record reliably establishes . . . [a] person as the person to which the transferable record was issued or transferred." § 201(b). A satisfactory system must produce a single authoritative copy of the record which:

(1) cannot be altered;
(2) can identify the person to whom the record was issued; and
(3) is maintained by the person asserting control over the record.

Further, any change in assignee of the authoritative copy can only be made with the consent of the person asserting control, and any copy of the authoritative copy must be easily identifiable as a copy. Additionally, any revision in the authoritative copy must be identified as either authorized or unauthorized by the person asserting control. Finally, a person asserting control over a transferable record is also considered the holder under the UCC, and an obligor under a transferable record has the same rights and defenses as under the UCC.