D R A F T

FOR DISCUSSION ONLY

UNIFORM ELECTRONIC TRANSACTIONS ACT

NATIONAL CONFERENCE OF COMMISSIONERS

ON UNIFORM STATE LAWS

MEETING IN ITS ONE-HUNDRED-AND-SEVENTH YEAR
CLEVELAND, OHIO

JULY 24 – 31, 1998

UNIFORM ELECTRONIC TRANSACTIONS ACT

WITH PREFATORY NOTE AND REPORTER'S NOTES

The ideas and conclusions set forth in this draft, including the proposed statutory language and any comments or reporter's notes, have not been passed upon by the National Conference of Commissioners on Uniform State Laws or the Drafting Committee. They do not necessarily reflect the views of the Conference and its Commissioners and the

Drafting Committee and its Members and Reporters. Proposed statutory language may not be used to ascertain the intent or meaning of any promulgated final statutory proposal.

DRAFTING COMMITTEE ON
UNIFORM ELECTRONIC TRANSACTIONS ACT

PATRICIA BRUMFIELD FRY, Stetson University, College of Law, 1401 61st Street South, St. Petersburg, FL 33707, *Chair*
STEPHEN Y. CHOW, One Beacon Street, 30th Floor, Boston, MA 02108
KENNETH W. ELLIOTT, Suite 630, 119 N. Robinson Avenue, Oklahoma City, OK 73102
HENRY DEEB GABRIEL, JR., Loyola University, School of Law, 526 Pine Street, New Orleans, LA 70118
BION M. GREGORY, Office of Legislative Counsel, State Capitol, Suite 3021, Sacramento, CA 95814-4996
JOSEPH P. MAZUREK, Office of Attorney General, P.O. Box 201401, 215 N. Sanders, Helena, MT 59620
PAMELA MEADE SARGENT, P.O. Box 846, Abingdon, VA 24212
D. BENJAMIN BEARD, University of Idaho, School of Law, 6th and Rayburn Streets, Moscow, ID 83844-2321, *Reporter*

EX OFFICIO

GENE N. LEBRUN, P.O. Box 8250, 9th Floor, 909 St. Joseph Street, Rapid City, SD 57709, *President*
HENRY M. KITTLESON, P.O. Box 32092, 92 Lake Wire Drive, Lakeland, FL 33802-2092, *Division Chair*

AMERICAN BAR ASSOCIATION ADVISORS

C. ROBERT BEATTIE, 150 S. 5th Street, Suite 3500, Minneapolis, MN 55402, *Business Law Section*
AMELIA H. BOSS, Temple University, School of Law, 1719 N. Broad Street, Philadelphia, PA 19122, *Advisor*
THOMAS J. SMEDINGHOFF, 500 W. Madison Street, 40th Floor, Chicago, IL 60661-2511, *Science and Technology Section*

EXECUTIVE DIRECTOR

FRED H. MILLER, University of Oklahoma, College of Law, 300 Timberdell Road, Norman, OK 73019, *Executive Director*
WILLIAM J. PIERCE, 1505 Roxbury Road, Ann Arbor, MI 48104, *Executive Director Emeritus*

Copies of this Act may be obtained from:

NATIONAL CONFERENCE OF COMMISSIONERS

ON UNIFORM STATE LAWS
211 E. Ontario Street, Suite 1300
Chicago, Illinois 60611
312/915-0195

UNIFORM ELECTRONIC TRANSACTIONS ACT

TABLE OF CONTENTS

UNIFORM ELECTRONIC TRANSACTIONS ACT

PREFATORY NOTE

1. History and Background

In June 1996, Commissioner Patricia Brumfield Fry submitted two memoranda to the Scope and Program Committee of the National Conference of Commissioners on Uniform State Laws (NCCUSL). The first memorandum outlined then existing digital signature statutes [Utah, Florida and California primarily], briefly explained digital signature technology, and furnished illustrations of writing and signature requirements in completed Uniform Acts, along with an analysis of policies underlying those requirements.

The second memorandum contained proposals for several potential drafting projects relating to electronic transactions and communications. It outlined a variety of then pending international and domestic projects addressing electronic commerce, described completed and pending NCCUSL projects relating to electronic commerce, and proposed two projects.

These memoranda were reviewed by the Scope and Program and Executive Committees of NCCUSL at the August 1996 Annual Meeting. At the same time, the Conference had before it proposals from the Committee on the Law of Commerce in Cyberspace [Business Law Section, American Bar Association] for projects dealing with electronic commerce, as well as reports on work under way in California, Oklahoma, Massachusetts and Illinois. As a result of its review of these materials, a Drafting Committee was approved "to draft an act consistent with but not duplicative of the Uniform Commercial Code, relating to the use of electronic communications and records in contractual transactions." The Drafting Committee was instructed to report to the Scope and Program Committee, at its January 1997 meeting, with a detailed outline of the proposed Act. Commissioner Fry was designated chair of the Drafting Committee. Professor D. Benjamin Beard, University of Idaho College of Law, was named reporter for the project.

Pursuant to its instructions, the new Drafting Committee and reporter reviewed and discussed, both in draft form and in conference calls, a number of draft memoranda dealing with the scope of the proposed Act. They were assisted in these efforts by the Ad Hoc Task Force on Electronic Contracting, formed by the American Bar Association and chaired by James E. Newell. [This Task Force was the precursor for the American Bar Association's Ad Hoc Committee on Uniform State Law on Electronic Contracting, which is participating in the drafting process and is charged ultimately with making recommendations to the A.B.A. concerning the .] Ultimately the Drafting Committee submitted its memorandum dated January

3, 1997 to the Scope and Program Committee. That memorandum stated that the fundamental goal of the project was to draft "such revisions to general contr law as are necessary or desirable to support transion processes utilizing existing and future electronic or computerized technologies." It further concurred in the general principles stated in the Committee's memorandum to guide decisions concerning both the content of the draft and expression of its provisions, including preservation of freedom of contr, technology-neutrality and technology-sensitivity, minimalism, and avoidance of regulation. The Committee was directed to make efforts to involve both technology and non-technology interests.

Based on these materials, the drafting project was authorized to proceed. The Drafting Committee has met four times. At the first meeting of the Drafting Committee in May 1997, time was devoted to learning about existing technologies and to assisting the reporter with a broad discussion of the nature and content of the provisions which should be included in the proposed Act. The Committee reviewed a set of provisions compiled by the reporter from other models.

At the August 1997 Annual Meeting, proposals were considered by the Scope and Program Committee relating to the use of electronic technologies by governmental entities. Commissioner Fry was asked to participate in the discussion of these proposals. Ultimately, the Scope and Program Committee and Executive Committee asked the Drafting Committee to include in the project treatment of public communications and transactions. In addition, the name of the project was changed from The Uniform Electronic Records and Communications in Contractual Transactions Act to the simpler Uniform Electronic Transactions Act.

The first draft was prepared for the second meeting of the Drafting Committee, held in September 1997 in Alexandria, Virginia. Three primary issues emerged from the Drafting Committee's consideration of the first draft. First, it became apparent that the scope of the Act would be a major issue. The first draft limited the applicability of the Act to electronic records and signatures used in commercial and governmental transactions, subject to a limited, and at that time, yet to be determined, set of excluded transactions. Secondly, the Drafting Committee began articulating the policy that this Act should be a procedural statute, affecting the underlying substantive law of a given transaction only if absolutely necessary in light of the differences in the media used. Finally, the Committee began to consider the extent to which the Act should or should not provide heightened legal protection for electronic records and signatures which have been created and used in conformity with security procedures which demonstrate greater reliability.

In each of the two succeeding drafts, the Committee worked to clarify the Scope provisions, eliminate unnecessary provisions considered to have a substantive impact on the underlying transaction, and ultimately to remove any legal protection

for so-called "secure" electronic signatures and records. This latest development has raised a fourth issue relating to the fundamental purpose and effect of a signature.

2. Citation and Style Notes.

Unless otherwise noted, references in this draft are to the following sources:

1. "Article 2B Draft" – Draft Uniform Commercial Code Article 2B – Licenses, March 1998.

2. "Illinois Model" – Illinois Electronic Commerce Security Act, December 15, 1997 Draft.

3. "Uncitral Model" – United Nations Model Law on Electronic Commerce, approved by the UN General Assembly November, 1996.

4. "Oklahoma Model" – Oklahoma Bankers Association Technology Committee, Digital Writing and Signature Statute, Second Discussion Draft, June 17, 1996.

5. "Massachusetts Model" – Massachusetts Electronic Records and Signatures Act, DRAFT – November 4, 1997.

6. "UCC Section" – Uniform Commercial Code, Official Text, 1990.

7. "Article 1 Draft" – Uniform Commercial Code Revised Article 1 – General Provisions (199_), September 1997 Draft.

Some sections and subsections appear in this draft in brackets. The Notes indicate that these provisions have been questioned by the Style Committee, but have not been reviewed by the Drafting Committee in light of the Style Committee's concerns. Accordingly they have been retained for discussion by the Drafting Committee at its meeting in October, 1998.

3. Principal Issues in the Draft. As noted above, three principal issues have evolved over the course of the Committee's three meetings this past year: (1) scope of the Act and procedural approach; (2) the level of heightened protection to be accorded electronic records and signatures; and (3) evolution of the concept and effect of a signature. One other issue has yet to be fully addressed by the Committee and that relates to the continuing propriety of the concept of manifestation of assent.

A. Scope of the Act and Procedural Approach. The scope of this Act remains one of the most difficult areas to be resolved by the Drafting Committee. However, the Committee has taken some strong positions over the course of the past year. Interestingly, the approach coming out of the Committee may be viewed as both expanding the coverage of the Act while simultaneously narrowing its effect.

With regard to the specific scope of the Act, the Committee, at the January 1998 meeting, voted to eliminate references to commercial and governmental transactions. Instead, the Act now will apply to *all* electronic records and electronic signatures unless specifically excluded in Section 104. A Task Force was formed to review sample state legislative compilations to determine which documents and records or transaction types should be excluded from the Act. The work of the Task Force is continuing and still in progress. Hopefully, the Task Force will have a report for the Committee in time for the results of that report to be reflected in the Draft to be discussed at the Committee's upcoming meeting in October, 1998.

While the overall coverage of the Act can be viewed as expanded by the Committee's approach to scope, the Committee has made clear over the course of the three meetings, that this Act is fundamentally a procedural statute to validate and effectuate transactions accomplished through an electronic medium. Through the limitation on the definition of agreement, the elimination of usage evidence factors in construing agreements, and the elimination of a specific obligation of good faith, the Committee has indicated its intent to leave these areas to resolution under the substantive law applicable to a given transaction.

B. The Extent of Heightened Legal Protection for Electronic Records and Signatures When Security Procedures Are Employed. The question of what, if any, heightened protection should be accorded electronic records and signatures where security procedures are applied, occupied much discussion at all three meetings. While a number of participants have argued that fairly strong presumptions are necessary to promote electronic commerce, others felt that the state of technology and current market was still too under-developed to warrant the creation of any presumptions. This draft reflects the decision of the Drafting Committee at its last meeting in April 1998, to delete all presumptions from this Act.

Until the April meeting, all drafts had provided for limited, "bursting bubble," rebuttable presumptions, in the context of electronic records and electronic signatures verified by the application of commercially reasonable security procedures. This approach was consistent with the treatment of presumptions under the current Uniform Commercial Code, and, more immediately, to the treatment of electronic signatures and records involving "attribution procedures" under Article 2B. The effect of such "soft" presumptions would require the party against whom the presumption operates to deny expressly the existence of the presumed fact.

Such a denial would be sufficient evidence to burst the bubble. At the same time, in cases where one establishes that a commercially reasonable procedure was used, even in the face of a denial, the logical inference to be drawn from the evidence of the security procedure, its "robustness" and efficacy, may well be sufficient to convince a jury that the record or signature is as claimed.

The principal arguments made in favor of the elimination of presumptions included the following:

1. The creation of statutory presumptions is not appropriate in the absence of certainty and stability regarding the predicate facts giving rise to the presumption. In this case, the certainty regarding the "robustness" of any given security procedure is lacking given the rapid pace of technological development. As one observer with technical expertise noted, in light of rapidly changing technology, it would be difficult, 2 years after a transaction, to state what was commercially reasonable and robust under the circumstances existing at the time of the transaction.

2. Given the uncertainty resulting from rapid technological development, it was not suggested that the presumption be strengthened to one which would shift the ultimate burden of persuasion, as is provided under the draft Uniform Rules of Evidence. At the same time, considered the existing "bursting bubble" presumption was so weak as to be largely meaningless.

3. By providing for presumptions in the electronic arena, the concern existed that a new regime would be created which might result in parties selecting a medium for a transaction based on the different legal effects. This would result in a fundamental shift from the policy of this Act to validate and effectuate electronic media in a way making it the equivalent of written media.

4. This Act currently does not make distinctions based on consumer/merchant, sophisticated/unsophisticated parties. The provisions of Section 110 on imposition of commercially unreasonable security procedures are intended to protect unsophisticated parties. However, in the absence of an imposition, the presence of a commercially reasonable procedure, and the fact that the relying party will normally be a vendor or other party choosing the media, the need for consumer protections is minimized, if not avoided. However, the possible creation of presumptions would operate to work against the interests of consumer and other unsophisticated parties.

5. In the international fora considering electronic commerce, it has become apparent that other legal systems attach greater significance to presumptions than was intended in this Act. Specifically, the concern was raised that the creation of

presumptions would provide a ground for governmental regulation in other countries, which was viewed as undesirable.

Notwithstanding these points, those favoring the creation of presumptions focused on a belief that the UETA should go beyond merely validating and effectuating electronic commerce, to actually promoting it. These people pointed to the necessity to deal with the issue of the effect of records and signatures in the electronic environment and what, if anything, would replace presumptions.

C. Evolution of the Concept and Effect of a Signature.

Particularly at the April, 1998 meeting, the concerns regarding the propriety of presumptions focused discussion on the effect properly to be accorded to a signature under existing law. A written signature on paper may serve one or more of the following purposes, among others:

- identification of a person
- verification of the party creating or sending the record
- verification of the informational integrity of the record
- acceptance or adoption of a term or record
- verification of a party's authority
- acknowledgement of receipt.

A recurring theme throughout the Committee's deliberations has been the recognition that the actual effect to be accorded to a given signature requires a consideration of all the facts and circumstances, i.e., the context, surrounding the execution of the signature.

Early on the Committee determined to use the term signature, as opposed to the term "authenticate" used in Article 2B. However, the Committee incorporated into early definitions of signature the attributes of identity, adoption and informational integrity appearing in the Article 2B definition of authenticate. This was considered merely a "fleshing-out" of the term "authenticate" as used in the current definition of signature in the Uniform Commercial Code.

With the deletion in April of the specific provisions in Section 302 outlining the effect of a signature because they were considered too narrow, a reconsideration of the definition and effect of a signature was required. This draft reflects the reporter's attempt to deal with that issue. Based on discussions at the April meeting, and subsequent correspondence, the one clear purpose of every signature seems to be that of identification. Therefore the definition of signature has been limited to identifying symbols. The requisite volition in applying such an identifying symbol is conveyed by the requirement that a person must "execute or adopt" a symbol. Then in Section 302, the effect of that symbol as a signature is left to other

law or the agreement of the parties. This approach is consistent with the Committee's sense that, unless absolutely necessary, this Act should not effect existing substantive law.

D. Agreement and Manifestation of Assent.

The concepts of manifestation of assent and opportunity to review have been retained as substantive sections in Part 1. While the definition of agreement no longer expressly includes manifestation of assent and now reflects the definition set forth in the UCC, the concept remains important in determining the terms of an agreement. Section 107 is intended to make the provision more of a procedural, "how to" provision. That is, where parties need to demonstrate agreement, one manner of doing that would be through showing a "manifestation of mutual assent" in the words of the Restatement.

Section 107 has been retained as a provision which would indicate how such a manifestation might be accomplished in an electronic transaction. Should not a person be deemed to have signed an order for goods or services over the internet even if no actual "signature" is attached to the transmission? By pointing and clicking on various terms and icons in order to obtain the goods or services, does not a person manifest the requisite intention to identify him/herself, adopt the terms clicked and agree to be bound by her/his actions? The Drafting Committee has not directly addressed the propriety of this concept in the UETA, and it has been retained for future discussion by the Committee. It is intended to track Article 2B in substance.

UNIFORM ELECTRONIC TRANSACTIONS ACT

PART 1
GENERAL PROVISIONS

SECTION 101. SHORT TITLE. This [Act] may be cited as the Uniform Electronic Transactions Act.

SECTION 102. DEFINITIONS.

(a) In this [Act] [unless the context otherwise requires]:

(1) "Agreement" means the bargain of the parties in fact as found in their language or inferred from other circumstances. [Whether an agreement has legal consequences is determined by this [Act], if applicable, or otherwise by other applicable rules of law.]

(2) "Automated transaction" means a transaction formed or performed, in whole or in part, by electronic means or electronic records in which the acts or records of one or both parties are not reviewed by an individual as an ordinary step in forming a contract, performing under an existing contract, or fulfilling any obligation required by the transaction.

(3) "Computer program" means a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result. The term does not include informational content.

(4) “Contract” means the total legal obligation resulting from the parties’ agreement as affected by this [Act] and other applicable rules of law.

(5) “Electronic” means of or relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic , or similar capabilities.

(6) “Electronic device “ means a computer program or other electronic or automated means designed, programmed, or selected by a person to initiate or respond to electronic records or performances in whole or in part without review by an individual.

(7) “Electronic record” means a record created, stored, generated, received, or communicated by electronic means.

(8) “Electronic signature” means a signature in electronic form, attached to or logically associated with an electronic record.

(9) “ Governmental agency” means an executive[, legislative, or judicial] agency, department, board, commission, authority, institution, or instrumentality of this State or of any county, municipality, or other political subdivision of this State.

(10) “Information” means data, text, images, sounds, codes, computer programs, software, databases, or the like.

(11) “Informational content” means information that in its ordinary use is intended to be communicated to or perceived by a person in the ordinary use of the information.

(12) "Information processing system" means a system for creating, generating, sending, receiving, storing, displaying, or otherwise processing information.

(13) "Notify" means to communicate, or make available, information to another person in a form and manner appropriate or required under the circumstances.

(14) "Person" means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, agency, instrumentality, or public corporation, or any other legal or commercial entity.

(15) "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

[(16) "Rule of law" means a statute, regulation, ordinance, common-law rule, court decision, or other law enacted, established, or promulgated in this State, or by any agency, commission, department, court, or other authority or political subdivision of this State.]

(17) "Security procedure," means a procedure [or methodology,] established by law or regulation, or established by agreement, or knowingly adopted by each party, for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the informational content of an electronic record. The term includes a procedure that

requires the use of algorithms or other codes, identifying words or numbers, encryption, callback or other acknowledgment procedures, or any other procedures that are reasonable under the circumstances.

(18) "Sign" means to execute or adopt a signature.

(19) "Signature" means an identifying symbol, sound, process, or encryption of a record in whole or in part, executed or adopted by a person.

(20) "Term" means that portion of an agreement which relates to a particular matter.

(21) "Transferable record" means a record, other than a writing, that would be an instrument or chattel paper under [Article 9 of the Uniform Commercial Code] or a document of title under [Article 1 of the Uniform Commercial Code], if the record were in writing.

(22) "Writing" includes printing, typewriting, and any other intentional reduction of a record to tangible form. "Written" has a corresponding meaning.

(b) Other definitions applying to this [Act] or to specified sections thereof, and the sections in which they appear are:

"Inadvertent error". Section 204

"Requiring party". Section 110

Sources: Definitions in this Act have been derived from Uniform Commercial Code definitions, in particular Article 2B drafts, and from other models, specifically the UNCITRAL Model Law, Illinois Model, Oklahoma Model and Massachusetts Model.

1. **"Agreement."**

Committee Votes:

A. To delete the concept of manifestation of assent from the definition – By consensus (no formal vote) (Sept. 1997)

B. To delete course of performance, course of dealing and usage of trade: Committee 4 Yes – 2 No; Observers 6 Yes – 1 No. (Jan. 1998)

At the September, 1997 meeting, the definition of agreement which included terms to which a party manifested assent was rejected. The consensus of both the Committee and observers was that there was no need to separate manifestations of assent from the language and circumstances which comprise the bargain in fact of the parties as part of the definition of agreement. Rather the Reporter was directed to return to the definition of agreement in the Uniform Commercial Code. Accordingly, the definition in the November Draft was taken from the most recent revision to Article 1. At the January, 1998 meeting, the Committee more specifically defined the policy guiding this Act: the Act is a *procedural* act providing for the means to effectuate transactions accomplished via an electronic medium, and, unless absolutely necessary because of the unique circumstances of the electronic medium, the Act should leave all questions of substantive law to law outside this Act. In light of this principle the prior references to usage evidence as informing the content of an agreement was considered substantive, and therefore, best left to other law outside this Act.

The need for a definition of agreement was acknowledged largely because the existence of a security procedure, as defined below, often depends on the agreement of the parties. However, the facts and evidence which establish an agreement is intended to be left to other law, e.g., the Uniform Commercial Code, common law, etc.

Whether the parties have reached an agreement is determined by their express language and surrounding circumstances. The Restatement of Contracts § 3 provides that

> "An agreement is a manifestation of mutual assent on the part of two or more persons. A bargain is an agreement to exchange promises or to exchange a promise for a performance or to exchange performances."

The Uniform Commercial Code specifically includes in the circumstances from which an agreement may be inferred "course of performance, course of dealing and usage of trade . . ." as defined in the UCC.

The existence and content of an agreement under this Act is determined by the parties' language and surrounding circumstances. The relevant surrounding circumstances and the context of the transaction will inform the precise terms of any agreement. The second sentence of this definition makes clear that the substantive law applicable to an electronic transaction effectuated by this Act must be applied to determine those circumstances relevant in establishing the precise scope and meaning of the parties' agreement. This sentence has been bracketed in recognition of the Style Committee's view that the provision is substantive and should not be included in the definition. Considering the source of this provision in the UCC which has a 40-50 year history of construction, the provision has been retained for discussion by the Drafting Committee at its next meeting.

The Comment to this definition will make clear that, though derived from the UCC definition, there is no intent to affect the meaning of the term under the UCC or any other applicable law.

2. **"Automated Transaction."**

Committee Vote: To delete references to governmental and commercial: Committee 4 Yes (Chair broke tie) – 3 No; Observers 19 Yes – 1 No. (Jan. 1998)

Article 2B has conformed its terminology with this Act by adopting "automated transaction" in place of "electronic transaction." The definitions in each are conceptually the same. The definition in this Act is broader, going beyond contract formation to performances under a contract and other obligations accomplished by electronic means in a transaction, because of the diversity of transactions to which this Act may apply.

As with electronic devices, this definition addresses the circumstance where electronic records may result in action or performance by a party although no human review of the electronic records is anticipated. Section 401(a) provides specific contract formation rules where one or both parties do not review the electronic records.

3. **"Computer program."** This definition is from Article 2B. The term is used principally with respect to the definition of "electronic device" and "information."

4. **"Electronic."** This definition serves to assure that the Act will be applied broadly as new technologies develop. While not all technologies listed are technically "electronic" in nature (e.g., optical fiber technology), the need for a recognized, single term warrants the use of "electronic" as the defined term.

5. **"Electronic device."** This draft has replaced the term "electronic agent" from Article 2B, with the term "electronic device" in order to avoid connotations of agency. Comments have been made at the Drafting Committee meetings from members of the Committee and observers that the key aspect of this term is its function as a tool of a party. The concern has been expressed that the use of the term "agent" may result in a court applying principles of the law of agency which are not intended and are not appropriate.

An electronic device, such as a computer program or other automated means employed by a person, is a tool of that person. As a general rule, the employer of a tool is responsible for the results obtained in the use of that tool since the tool has no independent volition of its own. However, an electronic device by definition is capable, within the parameters of its programming, of initiating, responding or interacting with other parties or their electronic devices once it has been activated by a party, without further attention of that party. This draft contains provisions dealing with the efficacy of, and responsibility for, actions taken and accomplished by electronic devices in the absence of human intervention.

While this Act proceeds on the paradigm that an electronic device is capable of performing only within the technical strictures of its preset programming, it is conceivable that, within the useful life of this Act, electronic devices may be created with the ability to act autonomously, and not just automatically. That is, through developments in artificial intelligence, a computer may be able to "learn through experience, modify the instructions in their own programs, and even devise new instructions." Allen and Widdison, "Can Computers Make Contracts?" *9 Harv. J.L.&Tech 25* (Winter, 1996). If such developments occur, courts may construe the definition of electronic device accordingly, in order to recognize such new capabilities.

Section 303 and Section 401 make clear that the party that sets operations of an electronic device in motion will be bound by the records and signatures resulting from such operations. A party is bound by the actions of a computer program designed to act without human intervention, as well as electronic and automated means such as telecopy and facsimile machines used by a party.

6. **"Electronic record."** An electronic record is a subset of the broader defined term "record." Unlike the term "electronic message" used in Article 2B, the definition is not limited to records intended for communication, but extends to any information contained or transferred in an electronic medium. It is also used in this Act as a limiting definition in those provisions in which it is used.

Electronic means for creating, storing, generating, receiving or communicating electronic records include information processing systems, computer

equipment and programs, electronic data interchange, electronic mail, or voice mail, facsimile, telex, telecopying, scanning, and similar technologies.

7. **"Electronic signature."** As with electronic record, this definition is a subset of the broader defined term "signature." The purpose of the separate definition is principally one of clarity in extending the definition of signature to the electronic environment.

The key aspect of this definition lies in the necessity that the electronic signature be linked or logically associated with the electronic record. For example, in the paper world, it is assumed that the symbol adopted by a party is attached to or located somewhere in the same paper that is intended to be signed. These tangible manifestations do not exist in the electronic environment, and accordingly, this definition expressly provides that the symbol must in some way be linked to, or associated with, the electronic record being signed. This linkage is consistent with the regulations promulgated by the Food and Drug Administration. 21 CFR Part 11 (March 20, 1997).

A digital signature using public key encryption technology would qualify as an electronic signature, as would the mere appellation of one's name at the end of an e-mail message – so long as in each case the signer executed or adopted the symbol and it identified the signer.

8. **"Governmental agency."** Although the approach to the scope of this Act has been revised (See Notes to Section 103), this definition is important in the context of Part 5. The reference to legislative and judicial agencies, etc. has been bracketed for further discussion by the Drafting Committee, in light of comment from members of the Committee that these should not be included.

9. **"Informational Content."** This definition has been added to differentiate information in an electronic record, which includes all data forming part of an electronic record, with the informational content of an electronic record which is the portion of the electronic record intended actually to be used by a human being. An example from Article 2B establishing this distinction is the Westlaw user who uses the search program to retrieve a case. The search program would be information, but only the case retrieved would be informational content.

10. **"Information processing system."** This term is used in Section 402 regarding the time and place of receipt of an electronic record. It is somewhat broader than the Article 2B definition.

11. **"Notify."** As with the provisions on receipt in Section 402, a notice sent to a party must be in a proper format to permit the recipient to use and

understand the information. For example, sending a message to a recipient in the United States in Chinese would not suffice to notify the recipient of the content of the message, in the absence of proof that the recipient understood Chinese. Similarly, sending a notice in WordPerfect 7.0 may not be appropriate when many people do not have the capability to convert from that format. In such a case, a more universal format such as ASCII would be required.

12. **"Record."** This is the standard Conference formulation for this definition.

13. **"Rule of Law."** The definition is drafted broadly. It has been bracketed in recognition of the Style Committee's recommendation that it be deleted and the undefined term "law" be substituted. It has been retained for Drafting Committee consideration this Fall.

14. **"Security procedure."** Limiting security procedures to those which are either agreed to or knowingly adopted by parties or established by law or regulation eliminates much of the concern regarding the impact security procedures may have on unsophisticated parties. The effect of commercially unreasonable security procedures imposed by one party is addressed in Section 110. In such cases the party at risk is the party imposing the commercially unreasonable procedure. In this way, the party with the greatest incentive to assess the risk of proceeding in a transaction with commercially unreasonable procedures will bear the loss.

The key aspects of a security procedure include verification of an electronic signature in addition to verification of the identity of the sender, and assurance of the informational integrity, of an electronic record. The definition does not identify any particular technology. This permits the use of procedures which the parties select or which are established by law. It permits the greatest flexibility among the parties and allows for future technological development.

15. **"Signature."** At the September Drafting Meeting, the consensus of the Committee and observers was to go back to the definition of signature, and to delete the definition of "authenticate." Given the purpose of this Act to equate electronic signatures with written signatures, the sense was that retaining signature as the operative word would better accomplish that purpose. However, the idea of fleshing out the concept of authenticate present in the existing UCC definition of signature was thought to be wise. Therefore, the definitional concepts set forth in the definition of authenticate in Article 2B were carried into the definition of signature.

At the April 1998 meeting a good deal of discussion related to the propriety of delineating the specific functions of a signature. The Committee deleted from

Section 302 a provision establishing the specific effects of an electronic signature. The one critical aspect of a signature that was recognized was its purpose of identification. Accordingly, the definition has been revised to reflect the principal function of a signature as an identifying symbol. In addition, some volition must attach to application of a symbol and this is noted by the requirement that the symbol be "executed or adopted" by a person. The effect of the signature is left to the underlying substantive law in light of all the facts and circumstances. See Section 302. In short, the definition here reflects the bare minimum as to the function of a signature, with the substantive effect being treated in Section 302 and the substantive law underlying the transaction.

16. **"Term."** This definition has its principal significance in the context of manifestation of assent and opportunity to review. It is bracketed pending the Committee's determination of the status of those concepts in this Act.

17. **"Transferable record."** This definition is necessary in the event the Drafting Committee decides to retain the applicability of this Act to such records. See Section 405.

18. **"Writing."** This definition reflects the current UCC definition.

SECTION 103. SCOPE. Except as otherwise provided in Section 104, this [Act] applies to electronic records and electronic signatures that relate to any transaction.

Source: Section 103 (Nov. 25, 1997 UETA Draft); Section 103 of Revised Draft of Article 1.

Committee Votes:

1. To delete references to commercial and governmental transactions – Committee 4 Yes – 3 No (Chair broke tie) Observers 19 Yes – 1 No (Jan. 1998).
2. To incorporate supplemental principles as part of Scope section – Committee Yes Unanimous Observers 12 Yes – 0 No (Jan. 1998).
3. To delete reference to supplemental principles (April 1998)

Reporter's Note

1. The scope of the Act has been clarified by limiting its applicability to *electronic* records and adding electronic signatures. The underlying premise of this

section is that this Act applies to all electronic records and signatures unless specifically excluded by the next section.

2. At the May, 1997 meeting, the Drafting Committee expressed strong reservations about applying this Act to *all* writings and signatures, as is contemplated in the Illinois, Massachusetts and other models. These same reservations were again raised at the September Meeting. An attempt was made in the Nov. 1997 draft to address those concerns by limiting applicability of the Act to only those records and signatures arising in the context of a "commercial transaction" or "governmental transaction," as therein defined. However, the view of a majority of the Committee and most observers was that defining the terms "commercial transactions" and "governmental transactions" was not possible with any degree of precision. Rather, a specific delineation of excluded transactions in the next section was considered preferable to an attempt to redefine commercial and governmental transactions.

3. In order to identify the specific transactions and transaction types to be excluded, a Task Force comprised of a number of observers and the Chair and Reporter for the Committee was formed under the leadership of R. David Whittaker. This Task Force was charged with reviewing selected statutory compilations (Massachusetts and Illinois being two States where significant work had already been started) to determine the types of transactions requiring writings and manual signatures which should be excluded from the coverage of this Act.

4. Section 104 will set forth specific exclusions to the coverage of this Act based on the work of the Task Force. As of the finalization of this Draft, however, that work was still in progress. Exclusions from the coverage of this Act will be set forth in a single section.

SECTION 104. EXCLUDED TRANSACTIONS.

(a) This [Act] does not apply to:

(1) [List of transactions identified by ETA Task Force on excluded transactions]; and

(2) transactions specifically excluded by any governmental agency under Part 5 .

(b) A transaction subject to this [Act] is also subject to:

(1) [the Uniform Commercial Code]; and

(2) [OTHER].

(c) The provisions of this [Act] and a rule of law referenced in subsection (b) must be construed whenever reasonable as consistent with each other. If such a construction is unreasonable a rule of law referenced in subsection (b) governs.

Source: New

Committee Vote: To delete "repugnancy" language, and provide that Act will apply except for specific exclusions. Committee 4 Yes – 1 No Observers 14 Yes – 1 No (with a number of abstentions)

Reporter's Note

This section reflects the Committee's position that, unless excluded, this Act will apply to all electronic records and signatures used in any transaction. Subsection (a) will set forth specific areas of law/transaction types to which this Act will not apply. This listing will be developed from the work of the Task Force formed at the January, 1998 meeting to review selected statutory compilations in order to identify candidates for exclusion.

In the March, 1998 Draft, the Uniform Commercial Code had been included in subsection (a) as excluded from the operation of this Act. The reporter was directed to revise the section to allow the application of this Act to the Uniform Commercial Code except where the two Acts conflict, in which case the UCC would apply. This approach is in accord with the charge from the Scope and Program Committee to draft a statute consistent, and not in conflict, with the UCC.

SECTION 105. VARIATION BY AGREEMENT.

(a) Except as otherwise provided in subsections (b) and (c), as between parties involved in generating, storing, sending, receiving, or otherwise processing or using electronic records or electronic signatures, provisions of this [Act] may be varied by agreement.

(b) The determination of commercial reasonableness in Section 109 may not be varied by agreement.

(c) The effect of requiring a commercially unreasonable security procedure stated in Section 110 may not be varied by agreement.

[(d) The presence in certain provisions of this [Act] of the words "unless otherwise agreed", or words of similar import, does not imply that the effect of other provisions may not be varied by agreement under subsection (a).]

(e) This [Act] does not require that records or signatures be generated, stored, sent, received, or otherwise processed or used by electronic means or in electronic form.

Source: UCC Section 1-102(3); Illinois Model Section 103.

Reporter's Note

1. Given the principal purpose of this Act to validate and effectuate the use of electronic media, it is important to preserve the ability of the parties to establish their own requirements concerning the method of generating, storing and communicating with each other. This Act affects substantive rules of contract law in very limited ways (See especially Part 4), by giving effect to actions done electronically. Even in those cases, the parties remain free to alter the timing and effect of their communications.

The only provisions of the Act which may not be disclaimed by agreement are those establishing the method and manner of determining the commercial reasonableness of a security procedure, and determining the effect of an imposed agreement to be bound by the results of a commercially unreasonable security procedure.

2. Subsection (d) has been bracketed for the Drafting Committee's consideration at its Fall meeting in light of the Style Committee's recommendation that the subsection be deleted.

3. Subsection (e) makes clear that this Act is intended to permit the use of electronic media, but does *not require* any person to use electronic media. For

example, if Chrysler Corp. were to issue a recall of automobiles via its internet website, it would not be able to rely on this Act to validate that notice in the case of a person who never logged on to the website, or indeed, had no ability to do so. The provisions in Sections 201(c) and 301(c) permitting a person to establish *reasonable* forms for electronic records and signatures assumes a pre-existing relationship between parties to a transaction, in which one party places reasonable limits on the records and signatures, electronic or otherwise, which will be acceptable to it.

SECTION 106. APPLICATION AND CONSTRUCTION. This [Act] must be construed liberally and applied consistently with commercially reasonable practices under the circumstances and to promote its purposes and policies.

Source: UCC Section 1-102

Reporter's Note

The following commentary, derived from the Illinois Electronic Commerce Security Section 102, has been moved from the text of Section 103 in the August Draft.

The purposes and policies of this are

(a) to facilitate and promote commerce and governmental transions by validating and authorizing the use of electronic records and electronic signatures;

(b) to eliminate barriers to electronic commerce and governmental transactions resulting from uncertainties relating to writing and signature requirements;

(c) to simplify, clarify and modernize the law governing commerce and governmental transactions through the use of electronic means;

(d) to permit the continued expansion of commercial and governmental electronic practices through custom, usage and agreement of the parties;

(e) to promote uniformity of the law among the States (and worldwide) relating to the use of electronic and similar technological means of effecting and performing commercial and governmental transactions;

(f) to promote public confidence in the validity, integrity and reliability of electronic commerce and governmental transactions; and

(g) to promote the development of the legal and business infrastructure necessary to implement electronic commerce and governmental transactions.

SECTION 107. MANIFESTING ASSENT. In a transaction governed by this [Act], the following rules apply:

(1) A person or electronic device manifests assent to a record or term if, acting with knowledge of, or after having an opportunity to review, the record or term it:

(A) signs the record or term; or

(B) engages in affirmative conduct or operations that the record clearly provides or the circumstances, including the terms of the record, clearly indicate will constitute acceptance, and the person or electronic device had an opportunity to decline to engage in the conduct or operations.

(2) Unless the substantive rules of law governing the transaction provide otherwise, mere retention of information or a record without objection is not a manifestation of assent.

(3) If assent to a particular term is required by the substantive rules of law governing the transaction, a person or electronic device does not manifest assent to the term unless there was an opportunity to review the term and the manifestation of assent relates specifically to the term.

(4) A manifestation of assent may be proved in any manner, including showing that a procedure existed by which a person or an electronic device must have engaged in conduct or operations that manifested assent to the record or term in order to proceed further in the transaction.

Source: Article 2B Draft Section 2B-111.

Reporter's Note

At the January, 1998 meeting express reference to manifestation of assent was removed from the substantive provisions of this Act where it had appeared. The section has been retained for further discussion in light of comment at the January meeting that it may be appropriate to retain the section as a procedural provision. The idea is to retain the concept in a way which indicates "how," in an electronic environment, parties may show manifestation of assent to a record or term. In light of the Committee's desire to leave the determination of what amounts to agreement to other, substantive law, it seems appropriate to establish a method outlining the manner in which parties can establish the "manifestation of mutual assent" referenced in Restatement 2d Contracts Section 3.

This section, together with the following section on "opportunity to review," provides a framework for the manner in which parties may establish agreement to a record or term when that agreement is undertaken electronically. Because of the nature of electronic media, it may well be the case that a party does not deal with a human being on the other side of a transaction.

In an electronic environment where computers are often pre-programmed and operate without human review of the operations in any particular, discreet transaction, it is not always the case that two humans have reached a "bargain in fact," i.e., a "meeting of the minds." Rather, the agreement is often the result of one party or its electronic device manifesting assent to terms or records presented to it on a "take it or leave it (i.e., exit)" basis, similar to the presentation of a standard form document in the paper environment.

The situations where parties participate in detailed negotiations leading to the formation of an integrated contract setting forth all the terms to which both parties have agreed are largely limited to transactions involving large amounts. Even outside the electronic environment, the use of pre-printed standard forms has supplanted detailed negotiations in many small amount transactions. Accordingly the concept of manifesting assent to a record or terms of a record has supplemented the notion of actual agreement in determining that to which the parties have agreed

to be bound (See Restatement (Second) Contracts Section 211, UCC Section 2-207).

Even in an electronic environment it remains possible to negotiate to agreement. In such a case, if parties engage in e-mail correspondence which results in a classic offer and acceptance of the terms (and only the terms) set forth in the correspondence, the electronic signatures appended to the e-mail messages may serve to authenticate the records and result in contract formation.

Contrasted with such a negotiated electronic contract is the situation where one calls up a provider on the Internet. The person determines to purchase the goods or services offered and is walked through a series of displayed buttons requesting the purchaser to agree to certain terms and conditions in order to obtain the goods and services. With each click on screen, the purchaser is indicating assent to that term in order to obtain the desired results. So long as the action of clicking in each case relates to a discreet term, or follows the full presentation of all terms, the actions of the purchaser can be said to clearly indicate assent to the terms available for review. As with the exchange of standard paper forms, there is no requirement that the terms be read before the on screen click occurs, so long as they were available to be read. Indeed, in such a scenario the problem of additional and conflicting terms which have so confused courts in the battle of the forms is not present.

A provision dealing with manifesting assent is particularly useful in the electronic environment where the real possibility of a contract being formed by two machines exists. The concept remains applicable in determining when a signature occurs and what the terms of an agreement are when contracts or signatures result from the operations of electronic devices, either between electronic devices or when interacting with a human.

SECTION 108. OPPORTUNITY TO REVIEW. A person or electronic device has an opportunity to review a record or term only if it is made available in a manner that:

(1) would call it to the attention of a reasonable person and permit review; or

(2) in the case of an electronic device, would enable a reasonably configured electronic device to react to it.

Source: Article 2B Draft Section 2B-112(a).

Reporter's Note

See Reporter's Note to Section 107, Manifesting Assent, *supra*.

SECTION 109. DETERMINATION OF COMMERCIALLY REASONABLE SECURITY PROCEDURE.

(a) The commercial reasonableness of a security procedure is determined by the court as a matter of law.

(b) In determining the commercial reasonableness of a security procedure, the following rules apply:

(1) A security procedure established by law is commercially reasonable for the purposes for which it was established.

(2) Except as otherwise provided in paragraph (1), commercial reasonableness is determined in light of the purposes of the procedure and the commercial circumstances at the time the parties agreed to or adopted the procedure, including the nature of the transaction, sophistication of the parties, volume of similar transactions engaged in by either or both of the parties, availability of alternatives offered to but rejected by a party, cost of alternative procedures, and procedures in general use for similar transactions.

(3) A commercially reasonable security procedure may require the use of any security measures that are reasonable under the circumstances.

Source: Article 2B Draft Section 2B-114.

Reporter's Note

This section separates the issue of the commercial reasonableness of a security procedure from the issue of the effect of imposition of a commercially unreasonable security procedure in the next section. This permits exclusion of the terms of this section from the general rule under this draft that the terms of this Act may be varied by agreement (Section 105).

SECTION 110. EFFECT OF REQUIRING COMMERCIALLY UNREASONABLE SECURITY PROCEDURE.

(a) If a person (the "requiring party") imposes, as a condition of entering into a transaction with another person, a requirement that the parties agree to be bound by the results of a security procedure that is not commercially reasonable, the following rules apply:

(1) (A) If the other party reasonably relies to its detriment on an electronic record or electronic signature purporting to be that of the requiring party and;

(B) application of the security procedure verified

(i) the source of the electronic record or electronic signature; or

(ii) the integrity of the informational content of the electronic record, the requiring party is estopped to deny the source, or integrity of the informational content, of the electronic record or electronic signature to which the security procedure was applied.

(2) If the requiring party relies on an electronic record or electronic signature purporting to be that of the other party, the other party retains the right to

deny the source of the electronic record or electronic signature, or the integrity of the informational content of the electronic record.

(b) A person does not impose a security procedure under subsection (a) if it makes commercially reasonable alternative security procedures available to the other person.

Source: New – based on consultation between the Article 2B Reporter and Committee Chair and the UETA Reporter and Committee Chair.

Reporter's Note

General Policy: This section is intended to impose liability and create strong disincentives for the imposition of the use of security procedures which are not commercially reasonable. This section is intended to apply only in the case where the requiring party is in a position to, and in fact does, impose the use of the commercially unreasonable procedure. As noted in subsection (b), if the parties negotiate or jointly select a procedure, or have commercially reasonable alternatives available, this section would have no application. In such a case, or indeed in cases where no security procedure is used, resulting losses are allocated in accordance with the applicable substantive law outside this Act.

Structure: The language in subsection (a) is intended to make clear that there must be knowledge on the part of the party upon whom the procedure is imposed that the imposer mandates the particular procedure. An imposition falling within this section requires agreement by both parties with knowledge of the procedure, rather than mere adoption by using the procedure. If the imposing party offers alternatives, there would actually be no imposition, and this section would not apply (subsection (b)).

Where a person requires, as a condition of doing business, a security procedure which cannot be shown to be commercially reasonable, an imposition has occurred and losses resulting from the other party's detrimental reliance will be borne by the requiring person under this section. While preventing an imposing party from any benefits resulting from reliance on a commercially unreasonable procedure, this section leaves to the underlying substantive law applicable to the particular transaction, the actual determination of the type, amount and extent of recoverable losses. The following illustrations suggest the manner of the operation of this section.

The easy cases – The requiring party is the recipient of the record:

Illustration 1. General Motors requires all franchisees to agree that any order received electronically and bearing only the franchisee's E-mail address as an identifier shall be attributable to, and binding upon, the franchisee identified. Since the franchisees are required by GM to do business in this way, this procedure would be an "imposed" procedure under this section.

Illustration 2. Same facts as Illustration 1. Through no fault of franchisee, bad guy sends an electronic record, showing franchisee's E-mail as the identifier, ordering $100,000 of merchandise from GM to be shipped to the bad guy. The procedure would not be commercially reasonable. If the underlying agreement as to the procedure were controlling, the franchisee would bear the loss, since the electronic record would be attributable to the franchisee. Since this is an imposed, commercially unreasonable procedure, the franchisee retains the right to deny that it sent the electronic record. Since GM would likely not be able to prove otherwise, the $100,000 loss arising directly from the transaction would be suffered by GM .

Illustration 3. Same facts as Illustration 2. If the bad guy is an employee of the franchisee the result, in this case, should be no different. The procedure is so open that the franchisee would have to somehow "lock up" all its computers to deny the employee the ability to send an order on behalf of the franchisee. Unless GM could establish attribution in fact under Section 202(a)(1) GM would bear the loss.

Illustration 4. Franchisee places a $100,000 order with GM. A bad guy hacks into GM's computer and learns of the order and the timing and method of shipment. The bad guy intercepts the shipment and steals it. While GM may be liable for negligence in the custody of its order records, this section is not applicable. Although there was a commercially unreasonable procedure, the loss in this case was not caused by the laxity of the procedure. If GM is able to prove that the order came from the franchisee the loss would be determined under Article 2 or general contract principles.

The more difficult cases – The requiring party is the sender of the record:

Illustration 5. GM requires all of its suppliers to do business using only GM's e-mail address as the identifier. Bad guy sends an e-mail showing GM's address as the identifier ordering $50,000 of parts. Supplier reasonably relies on the e-mail and ships the goods. Bad guy intervenes and takes the goods. In Supplier's claim for payment, GM will be estopped to deny that it sent the order. Without the ability to deny that the order was from GM, supplier may hold GM liable as though the contract had been formed, upon proof of supplier's performance, etc, under the substantive law of sales.

Illustration 6. Same procedure as in Illustration 5. GM actually sends order and supplier ships. As in Illustration 4, Bad guy learns of the shipment and intervenes and steals the shipment. Here the only question is risk of loss under applicable sales and contract law.

Illustration 7. In this case, GM has not required, as a condition of doing business, the use of any particular procedure. However, over a period of time, GM has placed and supplier has accepted purchase orders over open e-mail. Bad Guy sends a purchase order, purporting to be from GM, over open e-mail, and the supplier accepts and ships. This section does not apply. There has been no imposition by GM. Supplier is left to prove that the e-mail did come from GM, and upon failure to so prove, will bear any loss.

In a consumer context the general result will be that a vendor receiving an order will bear the risk that the order did not come from the purported sender. If a commercially reasonable security procedure is used by the vendor, the consumer would likely adopt the procedure in order to complete the transaction and the vendor would be able to prove the efficacy of the security procedure in order to establish consumer was the source of the order and should be bound. The following are somewhat atypical illustrations:

Illustration 8. Buyer writes e-mail to internet vendor indicating that the only way it will place an order is through use of a particular security procedure. The vendor writes back agreeing to the procedure. The procedure proves commercially unreasonable. In this case the buyer has imposed the procedure and will be estopped to deny the source or content of the electronic record. The result will be that the vendor may be able to enforce the terms of the record received upon proof of its content and the vendor's compliance with other requirements under sales or contract law.

Illustration 9. Buyer logs on to an internet vendor. In placing the order it uses a commercially unreasonable security procedure. Vendor has not agreed to the procedure but does adopt it by processing the order. This section does not apply. The parties are left to deny or prove up the resulting contract.

As indicated by the illustrations, the question of the extent of damage recovery by any party is left entirely to other law. The effect of a commercially unreasonable procedure that is imposed by one party is simply to raise estoppel or preserve rights of denial. After application of an estoppel, the transaction is proven or denied by other means and the resulting liability determined pursuant to other substantive law.

In the event that a transaction is accomplished without any security procedure, this Act, while validating the electronic records and signatures

implemented in transactions falling within the scope of this Act, does not address whether such records and signatures are otherwise legally binding or effective.

PART 2

ELECTRONIC RECORDS

SECTION 201. LEGAL RECOGNITION OF ELECTRONIC RECORDS.

(a) A record may not be denied legal effect, validity, or enforceability solely because it is an electronic record.

(b) If a rule of law requires a record to be in writing, or provides consequences if it is not, an electronic record satisfies the requirement .

(c) In a transaction, a person may establish reasonable requirements regarding the type of records acceptable to it.

Source: Sections 201 and 202 from UETA August Draft; Uncitral Model Articles 5 and 6; Illinois Model Sections 201 and 202.

Reporter's Note

1. Part 2 deals with those provisions relating to the validity, effect, and use of electronic records, Part 3 contains those sections dealing with the validity and effect of electronic signatures, and Part 4 reflects general contract provisions, and provisions dealing with the effect of both electronic records and electronic signatures. Under different provisions of substantive law the legal effect and enforceability of an electronic record may be separate from the issue of whether the record contains a signature. For example, where notice must be given as part of a contractual obligation, the effectiveness of the notice will turn on whether the party provided the notice regardless of whether the notice was signed. An electronic record attributed to a party under Section 202 would suffice in that case, notwithstanding that it may not contain a signature.

2. Subsection (a) establishes the fundamental premise of this Act: That the form in which a record is generated, presented, communicated or stored may not be the only reason to deny the record legal recognition. On the other hand, subsection (a) should not be interpreted as establishing the legal effectiveness, validity or enforceability of any given record. Where a rule of law requires that the record contain minimum substantive content, the legal effect, validity or enforceability will depend on whether the record meets the substantive requirements. However, the

fact that the information is set forth in an electronic, as opposed to paper record, is irrelevant.

3. Sections 201(a), 301(a), and 401(c), each provide for the non-discrimination against electronic media in the context of records, signatures and contract formation, respectively. Though some questions have been raised regarding the redundancy of these sections, they have been retained for clarity and certainty in assuring the validation and effectuation of electronic records and signatures in the specific context addressed by the respective sections.

4. Subsection (b) is a particularized application of subsection (a). Its purpose is to validate and effectuate electronic records as the equivalent of writings, subject to all of the rules applicable to the efficacy of a writing, except as such other rules are modified by the more specific provisions of this Act.

Illustration 1: A sends the following e-mail to B: "I hereby offer to buy widgets from you, delivery next Tuesday. /s/ A." B responds with the following e-mail: "I accept your offer to buy widgets for delivery next Tuesday. /s/ B." The e-mails may not be denied effect solely because they are electronic. In addition, the e-mails do qualify as records under the Statute of Frauds. However, because there is no quantity stated in either record, the parties' agreement would be unenforceable under existing UCC Section 2-201(1).

Illustration 2: A sends the following e-mail to B: "I hereby offer to buy 100 widgets for $1000, delivery next Tuesday. /s/ A." B responds with the following e-mail: "I accept your offer to purchase 100 widgets for $1000, delivery next Tuesday. /s/ B." In this case the analysis is the same as in Illustration 1 except that here the records otherwise satisfy the requirements of UCC Section 2-201(1). The transaction may not be denied legal effect solely because there is not a pen and ink "writing."

The purpose of the section is to validate electronic records in the face of legal requirements for paper writings. Where no legal requirement of a writing is implicated, electronic records are subject to the same proof issues as any other evidence.

5. Subsection (c) is a particularized application of Section 105, to make clear that parties retain control in determining the types of records to be used and accepted in any given transaction. For example, in the Chrysler recall hypothetical referred to in Note 2 to Section 105, although Chrysler cannot unilaterally require recall notices to be effective under this Act, it may indicate the method of recall in a purchase agreement with a customer. If the customer objects, the customer would have the right to establish reasonable requirements for such notices.

SECTION 202. ATTRIBUTION OF ELECTRONIC RECORD TO PARTY.

(a) An electronic record is attributable to a person if:

(1) it was in fact the action of the person, a person authorized by it, or the person's electronic device;

(2) another person, in good faith and acting in conformity with a commercially reasonable security procedure for identifying the person to which the electronic record is sought to be attributed, reasonably concluded that it was the act of the other person, a person authorized by it, or the person's electronic device.

(b) Attribution of an electronic record to a person under subsection (a)(2) has the effect provided for by law, regulation or an agreement regarding the security procedure.

Source: New – Originally derived from Article 2B Draft Section 2B-116.

Reporter's Note

This section sets forth rules establishing the circumstances under which a party will be bound by (be attributable for) an electronic record sent to another party.

Subsection (a)(1) relies on general agency law, including the use of electronic devices, to bind the sender. Subsection (a)(2) deals with attribution where security procedures are involved and properly implemented. Under subsection (a)(2) an electronic record will be attributed to the sender if the recipient complied, in good faith, with a commercially reasonable security procedure which confirmed the source of the electronic record. The legal effect and consequence of such attribution is left to other law or agreement under subsection (b).

SECTION 203. DETECTION OF CHANGES. If the parties act in conformity with a commercially reasonable security procedure to detect changes in the informational content of an electronic record, between the parties, the following rules apply:

(1) If a sender has conformed to the security procedure, but the other party has not, and the nonconforming party would have detected the change had that party also conformed, the sender is not bound by the change.

(2) If the other party notifies the sender in a manner required by the security procedure which describes the informational content of the record as received, the sender shall review the notification and report in a commercially reasonable manner any error detected by it. Failure so to review and report any error binds the sender to the informational content of the record as received.

Source: New – Originally derived from Article 2B Draft Section 2B-117

Reporter's Note

Like Section 202, this section allocates the risk of changes in transmission to the party that could have best detected the change through the proper application and use of a security procedure. Again, since the parties will have agreed or adopted the security procedure, allocation of risk to the party that should have discovered the error, should not pose undue hardship or unfair surprise on the party bearing the loss.

SECTION 204. INADVERTENT ERROR.

(a) In this section, "inadvertent error" means an error by an individual made in dealing with an electronic device of the other party if the electronic device of the other party did not allow for the correction of the error.

(b) In an automated transaction involving an individual, the individual is not responsible for an electronic record that the individual did not intend but which was caused by an inadvertent error if, on learning of the other party's reliance on the erroneous electronic record, the individual:

(1) in good faith promptly notifies the other party of the error and that the individual did not intend the electronic record received by the other party;

(2) takes reasonable steps, including steps that conform to the other party's reasonable instructions, to return to the other party or destroy the consideration received, if any, as a result of the erroneous electronic record; and

(3) has not used or received the benefit or value of the consideration, if any, received from the other party.

Source: UETA Section 203(c-e) (Nov. 1997 Draft) – Originally derived from Article 2B Draft.

Reporter's Notes

Section 2B-117(c) of the November 1,1997 draft of Article 2B created a new, rather elaborate defense for consumers when errors occur. As drafted the defense related to errors occurring because of system failures. Whether Article 2B addresses human error (as in the single stroke error of concern to a number of observers at the September Meeting) could be clearer, although the recent draft and Illustration 2 to that section, suggest that what is termed "inadvertent error" here is covered. Because the allocation of losses under this draft turns on the use of security procedures and their commercial reasonableness and places the loss on the party choosing to rely on electronic records and electronic signatures, the distinction between consumers and merchants, and sophisticated and unsophisticated parties has been eliminated. Rather the burden is placed on the person consciously desiring the benefits of electronic media to assure that the level of security necessary exists.

However, this section attempts to address the issue of human error in the context of an automated transaction. The reason for attempting to address this issue is that inadvertent errors, such as a single keystroke error, do occur, and are difficult, if not impossible to retrieve, given the speed of electronic communications.

However, the definition of "inadvertent error" would allow a vendor to provide an opportunity for the individual to confirm the information to be sent, in order to avoid the operation of this provision. By providing an opportunity to an individual to review and confirm the information initially sent, the other party can eliminate the possibility of the individual defending on the grounds of inadvertent error since the electronic device, through confirmation, allowed for correction of the error.

SECTION 205. ORIGINALS: ACCURACY OF INFORMATION.

(a) If a rule of law [or a commercial practice] 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 requirement is met by an electronic record if [the electronic record is shown to reflect accurately] [there exists a reliable assurance as to the integrity of] the information set forth in the electronic record after it was first generated in its final form, as an electronic record or otherwise.

(b) The integrity and accuracy of the information in an electronic record are determined by whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change arising in the normal course of communication, storage, and display. The standard of reliability required must be assessed in the light of the purpose for which the information was generated and in the light of all relevant circumstances.

Source: Former Section 205 (UETA Aug. Draft); Uncitral Model Article 8; Illinois Model Section 204.

Reporter's Note

This section deals with the serviceability of electronic records as originals. As was noted at the May, 1997 meeting, the concept of an original electronic document is problematic. For example, as I draft this Act the question may be asked

what is *the* "original" draft. My answer would be that the "original" is either on a disc or my hard drive to which the document has been initially saved. Since I periodically save the draft as I am working, the fact is that at times I save first to disc then to hard drive, and at others vice versa. In such a case the "original" may change from the information on my disc to the information on my hard drive. Indeed, as I understand computer operations, it may be argued that the "original" exists solely in RAM and, in a sense, the original is destroyed when a "copy" is saved to a disc or to the hard drive. In any event, the concern focuses on the integrity of the information, and not with its "originality." Given the recognition of this problem, the title of the section has been expanded to reflect the concern regarding the accuracy of the information in an electronic record; integrity which is assumed to exist in the case of an original writing.

A second question raised at the May, 1997 meeting related to when the law requires an "original." Except in the context of paper tokens such as documents of title and negotiable instruments, most requirements for "originals" derive from commercial practice where the assurance of informational integrity is a concern. The comment to Illinois Model Law Section 204 (derived largely from Uncitral Model Law Summary Paragraph 62) identifies some of these situations as follows:

> The requirement that a document be "an original" occurs in a variety of contexts for a variety of reasons. Documents of title and negotiable instruments, for example, typically require the endorsement and presentation of an original. But in many other situations it is essential that documents be transmitted unchanged (i.e., in their "original" form), so that other parties, such as in international commerce, may have confidence in their contents. Examples of such documents that might require an "original" are trade documents such as weight certificates, agricultural certificates, quality/quantity certificates, inspection reports, insurance certificates, etc. Other non-business related documents which also typically require an original form include birth certificates and death certificates. When these documents exist on paper, they are usually only accepted if they are "original" to lessen the chance that they have been altered, which would be difficult to detect in copies.

Since requirements for "originals" are often the result of commercial practice and not an actual rule of law, the section includes the bracketed language regarding requirements derived from commercial practice. As a policy matter it is not at all clear that legislation should override established commercial practice. This provision remains bracketed as a question which must be resolved by the Drafting Committee.

So long as there exists reliable assurance that the electronic record accurately reproduces the information, this section continues the theme of

establishing the functional equivalence of electronic and paper-based records. This is consistent with Fed.R.Evid. 1001(3) and Unif.R.Evid. 1001(3) (1974) which provide:

> If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original."

The bracketed alternatives for testing the reliability of the informational content of an electronic record have been retained for the Drafting Committee's consideration. At the May, 1997 meeting concern was expressed that the "reasonable assurance" standard was too vague. The first alternative tracks the language in the rules of evidence and focuses on the accuracy of the information presented. The second alternative is the language appearing in Section 204 of the Illinois Model.

Another issue relates to the use of originals for evidentiary purposes. In this context the concern principally relates to the "best evidence" or "original document" rule. The use of electronic records in evidence is addressed in Section 404 and its notes.

SECTION 206. RETENTION OF ELECTRONIC RECORDS.

(a) If a rule of law requires that certain documents, records, or information be retained, that requirement is met by retaining an electronic record, if:

(1) the information contained in the electronic record remains accessible for later reference;

(2) the electronic record is retained in the format in which it was generated, stored, sent, or received, or in a format that can be demonstrated to reflect accurately the information as originally generated, stored, sent, or received; and

(3) the information, if any, is retained in a manner that enables the identification of the source of origin and destination of an electronic record and the date and time it was sent or received.

(b) A requirement to retain documents, records, or information in accordance with subsection (a) does not extend to any information whose sole purpose is to enable the record to be sent or received.

(c) A person satisfies subsection (a) by using the services of any other person if the conditions set forth in subsection (a) are met.

(d) This section does not preclude a federal or state agency from specifying additional requirements for the retention of records, either written or electronic, subject to the agency's jurisdiction.

Source: Uncitral Model Article 10; Illinois Model Section 206.

Reporter's Note

At the May, 1997 meeting concern was expressed that retained records may become unavailable because the storage technology becomes obsolete and incapable of reproducing the information on the electronic record. Subsection (a)(1) addresses this concern by requiring that the information in the electronic record "remain" accessible, and subsection (a)(2) addresses the need to assure the integrity of the information when the format is updated or changed.

This section would permit parties to convert original written records to electronic records for retention so long as the requirements of subsection (a) are satisfied. Accordingly, in the absence of specific requirements to retain written records, written records may be destroyed once saved as electronic records satisfying the requirements of this section.

PART 3

ELECTRONIC SIGNATURES

SECTION 301. LEGAL RECOGNITION OF ELECTRONIC SIGNATURES.

(a) A signature may not be denied legal effect, validity, or enforceability solely because it is an electronic signature.

(b) If a rule of law requires a signature, or provides consequences in the absence of a signature, the requirement is satisfied with respect to an electronic record if the electronic record includes an electronic signature.

(c) In a transaction, a party may establish reasonable requirements regarding the method and type of signatures acceptable to it.

Source: Uncitral Model Article 7; Illinois Model Section 203(a); Oklahoma Model Section IV.

Reporter's Note

1. Subsection (a) establishes the fundamental premise of this Act: That the form in which a signature is generated, presented, communicated or stored may not be the *only* reason to deny the signature legal recognition. On the other hand, subsection (a) should not be interpreted as establishing the legal effectiveness, validity or enforceability of any given signature. Where a rule of law requires that a record be signed with minimum substantive requirements (as with a notarization), the legal effect, validity or enforceability will depend on whether the signature meets the substantive requirements. However, the fact that a signature appears in an electronic, as opposed to paper record, is irrelevant.

2. Subsection (b) is a particularized application of subsection (a). Its purpose is to validate and effectuate electronic signatures as the equivalent of pen and ink signatures, subject to all of the rules applicable to the efficacy and formality of a signature, except as such other rules are modified by the more specific provisions of this Act.

3. This section merely reiterates for clarity the rule that an electronic record containing an electronic signature satisfies legal requirements. The critical issue in either the signature or electronic signature context is what the signer intended by the execution, attachment or incorporation of the signature into the record. That question, under Section 302, is left to the underlying substantive law.

4. This section is technology neutral – it neither adopts nor prohibits any particular form of electronic signature. However, it only validates electronic signatures for purposes of applicable legal signing requirements and does not address the legal sufficiency, reliability or authenticity of any particular signature. As in the paper world, questions of the signer's intention and authority, as well as questions of fraud, are left to other law. The effect and proof of electronic signatures is addressed in the next section.

5. As in Section 201(c), subsection (c) preserves the right of a party to establish reasonable requirements for the method and type of signatures which will be acceptable. Accordingly, and consistent with Section 105, a party may refuse to accept any electronic signature and of course establish the method and type of electronic signature which is acceptable.

SECTION 302. EFFECT OF ELECTRONIC SIGNATURES.

(a) Except as provided in subsection (b), the effect of an electronic signature shall be determined from the context and surrounding circumstances at the time of its execution or adoption.

(b) As between parties to an agreement, the following rules apply:

(1) An electronic signature shall have the effect provided in the agreement.

(2) An electronic record containing an electronic signature is signed as a matter of law if the electronic signature is verified in conformity with a commercially reasonable security procedure for the purpose of verification of electronic signatures.

Source: New – Originally derived from Article 2B Draft Section 2B-118(a) and (c); Illinois Model Section 203.

Reporter's Note

1. An electronic signature is any identifying symbol or methodology executed or adopted by a person. This Act had included in the definition of signature the attributes normally associated with a pen and ink signature in order to make clear what a signer intends by *signing* a document, i.e., to identify oneself, adopt the terms of the signed record, and verify the integrity of the informational content of the record which is signed. At the April, 1998 meeting concern was expressed that these attributes were too exclusive because signatures may be used for other purposes as well. Consequently, the *effect* of the signature is left to agreement or other law.

2. Subsection (b)(2) provides that an electronic record is signed *as a matter of law* when a security procedure is used. However, this only establishes the fact of signature and not the effect to be given to an electronic signature.

SECTION 303. OPERATIONS OF ELECTRONIC DEVICES.

(a) A party that designs, programs, or selects an electronic device is bound by operations of the device.

(b) A party bound by the operations of an electronic device under subsection (a), is deemed to have signed an electronic record produced by the device on its behalf, whether or not the operations result in the attachment or application of an electronic signature to the electronic record.

Source: UETA Section 303 (March, 1998 Draft) – Originally derived from Article 2B.

Reporter's Note

1. This section extends signing to the electronic device, automated context. Its purpose is to establish that by programming an electronic device, a party assumes responsibility for electronic records and operations "executed" by the program. While the electronic device may or may not execute a symbol representing an electronic signature (i.e., with *present* human intent to authenticate the electronic

record), the party programming the electronic device has indicated its authentication of records and operations produced by the electronic device within the parameters set by the programming. Accordingly, the party should be bound and deemed to have signed the records of the electronic device. Again, the effect of such a signature is left to other law or agreement under Section 302.

PART 4

ELECTRONIC CONTRACTS AND COMMUNICATIONS

SECTION 401. FORMATION AND VALIDITY.

(a) In an automated transaction, the following rules apply:

(1) A contract may be formed by the interaction of electronic devices even if no individual was aware of or reviewed the electronic device's actions or the resulting terms and agreements. A contract is formed if the interaction results in the electronic devices' engaging in operations that confirm the existence of a contract or indicate agreement, such as by engaging in performing the contract, ordering or instructing performance, accepting performance, or making a record of the existence of a contract.

(2) A contract may be formed by the interaction of an electronic device and an individual. A contract is formed by the interaction if the individual performs actions that the individual knows or reasonably should know will cause the device to complete the transaction or performance, or which are clearly indicated to be an acceptance, regardless of other expressions or actions by the individual to which the individual cannot reasonably expect the electronic device to react.

(3) The terms of a contract resulting from an automated transaction include:

(A) terms of the parties' agreement;

(B) terms that the electronic device could take into account; and

(C) to the extent not covered by subparagraph (A) or (B), terms provided by law.

(b) If an electronic record initiated by a party or an electronic device evokes an electronic record in response and the electronic records reflect an intent to be bound, a contract is formed :

(1) when the response signifying acceptance is received; or

(2) if the response consists of electronically performing the requested consideration in whole or in part, when the requested consideration, to be performed electronically, is received unless the initiating electronic record prohibited that form of response.

(c) Unless otherwise agreed, a contract may not be denied legal effect, validity, or enforceability solely because an electronic record was used in its formation.

Source: Article 2B Draft Section 2B-204; Uncitral Model Article 11.

Reporter's Note

1. Subsection (a) addresses those transactions not involving human review by one or both parties and provides rules to expressly validate contract formation when electronic devices are involved. It sets forth the circumstances under which formation will occur in a fully automated transaction and under an automated transaction where one party is an individual.

2. Subsection (a)(2) addresses the circumstance of an individual dealing with an electronic device. This provision differs from the parallel provision of Article 2B-204.

As noted in a number of comments at the January, 1998 meeting, whether one knows that one is dealing with an electronic device should be irrelevant, so long as the individual proceeds with actions it knows or reasonably should know will result in accomplishment of the ends desired. Concerns previously expressed by

observers that individuals may not know what contemporaneous statements made by the individual would be given effect because of the possibility of contemporaneous or subsequent human review, have been addressed by limiting those actions of the individual which may result in a contract to those which the individual would reasonably expect to result in a contract. This will provide the party employing an electronic device with an incentive to make clear the parameters of the device's ability to respond. If the party employing the electronic device provides such information, the individual's act of proceeding on the basis of contemporaneous actions or expressions not within the parameters of the device would be unreasonable and such actions and expressions could not be the basis for contract formation.

3. Subsection (b) deals with timing in the formation of a contract by electronic means. Subsection (b)(2) makes clear that acceptance by performance, either in whole or in part, when the performance is electronic, occurs on receipt. When acceptance of an offer by performance occurs other than electronically (e.g. by the shipment of product), acceptance is governed by other rules of law such as the UCC and common law. As to timing of receipt see Section 402.

4. Subsection (c) makes clear that the use of electronic records, e.g., offer and acceptance, in the context of contract formation may not be the sole ground for denying validity to the contract. It is another particularized application of the general rules stated in Sections 201(a) and 301(a). At the request of one member of the Drafting Committee, the introductory clause has been added to confirm that the use of electronic records in this context may be avoided by agreement of the parties.

SECTION 402. TIME AND PLACE OF SENDING AND RECEIPT.

(a) Unless otherwise agreed between the sender and the recipient, an electronic record is sent when it enters an information processing system outside the control of the sender or of a person that sent the electronic record on behalf of the sender.

(b) Unless otherwise agreed between the sender and the recipient, an electronic record is received when the electronic record enters an information processing system from which the recipient is able to retrieve electronic records in a

form capable of being processed by that system, if the recipient uses or has designated that system for the purpose of receiving such an electronic record or information. An electronic record is also received when the recipient learns of its content.

(c) Subsection (b) applies even if the place the information processing system is located is different from the place the electronic record is considered to be received under subsection (d).

(d) Unless otherwise agreed between the sender and the recipient, an electronic record is deemed to be sent from the sender's place of business and is deemed to be received at the recipient's place of business. For the purposes of this subsection, the following rules apply:

(1) If the sender or recipient has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, if there is no underlying transaction, the principal place of business.

(2) If the sender or the recipient does not have a place of business, the place of business is the recipient's residence.

(e) Subject to Section 403, an electronic record is effective when received even if no individual is aware of its receipt.

Source: Article 2B Draft Section 2B-102(a)(36), and 2B-120(a); Uncitral Model Article 15.

Reporter's Note

1. This section provides default rules regarding when an electronic record is sent and when and where an electronic record is received. As with acknowledgments of receipt under Section 403, this section does not address the

efficacy of the record that is received. That is, whether a record is unintelligible or unusable by a recipient is a separate issue from whether that record was received.

2. Subsection (b) provides simply that when a record enters the system which the recipient has designated or uses and to which it has access, in a form capable of being processed by that system, it is received. Unless the parties have agreed otherwise, entry into any system to which the recipient has access will suffice. By keying receipt to a system which is accessible by the recipient, the issue of leaving messages with a server or other service is removed. However, the issue of how the sender proves the time of receipt is not resolved by this section. The last sentence provides the ultimate fallback by providing that in all events a record is received when the recipient has knowledge of it.

3. Subsections (c) and (d) provide default rules for determining where a record will be considered to have been received. The focus is on the place of business of the recipient and not the physical location of the information processing system. As noted in paragraph 100 of the commentary to the Uncitral Model Law

> It is not uncommon for users of electronic commerce to communicate from one State to another without knowing the location of information systems through which communication is operated. In addition, the location of certain communication systems may change without either of the parties being aware of the change.

Accordingly, where the place of sending or receipt is an issue, the relevant location should be the location of the sender or recipient and not the location of the information processing system.

4. Subsection (e) rejects the mailbox rule and provides that electronic records are effective on receipt. This approach is consistent with Article 4A and, as to electronic records, Article 2B.

SECTION 403. ELECTRONIC ACKNOWLEDGMENT OF RECEIPT.

(a) If the sender of a record requests or agrees with the recipient of the record that receipt of the record must be acknowledged electronically, the following rules apply:

(1) If the sender indicates in the record or otherwise that the record is conditional on receipt of an electronic acknowledgment, the record does not bind the sender until acknowledgment is received, and the record is no longer effective if acknowledgment is not received within a reasonable time after the record was sent.

(2) If the sender does not indicate that the record is conditional on electronic acknowledgment and does not specify a time for receipt, and electronic acknowledgment is not received within a reasonable time after the record is sent, the sender, upon notifying the other party, may:

(A) treat the record as being no longer effective; or

(B) specify a further reasonable time within which electronic acknowledgment must be received and, if acknowledgement is not received within that time, treat the record as being no longer effective.

(3) If the sender specifies a time for receipt and receipt does not occur within that time, the sender may treat the record as no longer being effective .

(b) Receipt of electronic acknowledgment establishes that the record was received but, in itself, does not establish that the content sent corresponds to the content received.

Source: Article 2B Draft Section 2B-120(b) and (c); Uncitral Model Article 14.

Reporter's Note

This section deals with functional acknowledgments as described in the ABA Model Trading Partner Agreement. The purpose of such functional acknowledgments is to confirm receipt, and not necessarily to result in legal consequences flowing from the acknowledgment.

Subsection (a) permits the sender of a record to be the master of its communication by requesting or requiring acknowledgment of receipt. The subsection then sets out default rules for the effect of the original message under different circumstances.

As noted in subsection (b) the only effect of a functional acknowledgment is to establish receipt. The acknowledgment alone does not affect questions regarding the binding effect of the acknowledgment nor the content, accuracy, time of receipt or other issues regarding the legal efficacy of the record or acknowledgment.

SECTION 404. ADMISSIBILITY IN EVIDENCE.

(a) In a legal proceeding, evidence of an electronic record or electronic signature may not be excluded:

(1) on the sole ground that it is an electronic record or electronic signature; or

(2) on the ground that it is not in its original form or is not an original.

(b) In assessing the evidentiary weight of an electronic record or electronic signature, the trier of fact shall consider the manner in which the electronic record or electronic signature was generated, stored, communicated, or retrieved, the reliability of the manner in which the integrity of the electronic record or electronic signature was maintained, the manner in which its originator was identified or the electronic record was signed, and any other relevant circumstances.

Source: UETA Section 206 (August Draft); Uncitral Model Article 9; Illinois Model Section 205.

Reporter's Note

Like Sections 201(a) and 301(a), subsection (a)(1) prevents the nonrecognition of electronic records and signatures solely on the ground of the media in which information is presented. Subsection (a)(2) also precludes inadmissibility on the ground an electronic record is not an original.

Nothing in this section relieves a party from establishing the necessary foundation for the admission of an electronic record. Subsection (b) gives guidance to the trier of fact in according weight to otherwise admissible electronic evidence.

SECTION 405. TRANSFERABLE RECORDS. If the identity of the person entitled to enforce a transferable record can be reliably determined from the record itself or from a method employed for recording, registering, or otherwise evidencing the transfer of interests in such records, the person entitled to enforce the record is deemed to be in possession of the record.

Source: Oklahoma Model Section III.B.2.

Reporter's Note

This section has been retained for discussion by the Drafting Committee on whether such documents should be covered by this Act.

The key to this section is to create a means by which a "holder" may be considered to be in possession of an intangible electronic record. If technological advances result in an ability to identify a single "rightful holder" of a negotiable instrument electronic equivalent, the last hurdle to holder in due course status would be possession, which this section would provide.

PART 5

GOVERNMENTAL ELECTRONIC RECORDS

SECTION 501. CREATION AND RETENTION OF ELECTRONIC RECORDS AND CONVERSION OF WRITTEN RECORDS BY GOVERNMENTAL AGENCIES. [Unless expressly prohibited by statute, each] [Each] governmental agency shall determine if, and the extent to which, it will create and retain electronic records instead of written records and convert written records to electronic records. [The [designated state officer] shall adopt rules governing the disposition of written records after conversion to electronic records.]

Source: Massachusetts Electronic Records and Signatures Act Section 3 (Draft – November 4, 1997)

Reporter's Note

See Notes following Section 504.

SECTION 502. RECEIPT AND DISTRIBUTION OF ELECTRONIC RECORDS BY GOVERNMENTAL AGENCIES.

(a) [Except as expressly prohibited by statute each] [Each] governmental agency shall determine whether, and the extent to which, it will send and receive electronic records and electronic signatures to and from other persons, and otherwise create, use, store, and rely upon electronic records and electronic signatures.

(b) In a case governed by subsection (a), the governmental agency, by appropriate regulation giving due consideration to security, [may] [shall] specify:

(1) the manner and format in which the electronic records must be created, sent, received, and stored;

(2) if electronic records must be electronically signed, 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 integrity, security, confidentiality, and auditability of electronic records; and

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

(c) All regulations adopted by a governmental agency must conform to the applicable requirements established by [designated state officer] pursuant to Section 503.

(d) This [Act] does not require any governmental agency to use or permit the use of electronic records or electronic signatures.

Source: Illinois Model Section 801; Florida Electronic Signature Act, Chapter 96-324, Section 7 (1996).

Reporter's Note

See Notes following Section 504.

SECTION 503. [DESIGNATED STATE OFFICER] TO ADOPT STATE STANDARDS. The [designated state officer] may adopt regulations setting forth rules, standards, procedures, and policies for the use of electronic records and electronic signatures by governmental agencies. If appropriate, those regulations must specify differing levels of standards from which implementing governmental agencies may choose in implementing the most appropriate standard for a particular application.

Source: Illinois Model Section 802(a).

Reporter's Note

See Notes following Section 504.

SECTION 504. INTEROPERABILITY. To the extent practicable under the circumstances, regulations adopted by [designated state officer] or a governmental agency relating to the use of electronic records or electronic signatures must be drafted in a manner designed to encourage and promote consistency and interoperability with similar requirements adopted by governmental agencies of other States and the federal government.

Source: Illinois Model Section 803.

Reporter's Note to Part 5

This Part addresses the expanded scope of this Act.

1. Section 501 is derived from former Section 501(a) and authorizes state agencies to use electronic records and electronic signatures generally for intra-governmental purposes, and to convert written records and manual signatures to electronic records and electronic signatures. By its terms it leaves the decision to use electronic records or convert written records and signatures to the governmental

agency. It also authorizes the destruction of written records after conversion to electronic form. In this regard, the bracketed language *requires* the appropriate state officer to issue regulations governing such conversions.

2. Section 502 covers substantially the same subject as former Section 501(b). It has been revised along the model of the pending Illinois legislation and broadly authorizes state agencies to send and receive electronic records and signatures in dealing with non-governmental persons. Again, the provision is permissive and not obligatory (see subsection (d)).

2. Section 502(c) requires governmental agencies, in adopting regulations for the use of electronic records and signatures to conform to standards established by the designated state officer under Section 503. The question here is whether the state agencies should be required, or merely permitted, to promulgate such regulations before accepting electronic records?

3. Section 503 authorizes a designated *state* officer to promulgate standards and regulations for the use of electronic media. The idea in this case is that a central authority should adopt broad standards and regulations which can be tailored consistently by individual governmental agencies to meet the needs of the particular agency. Should the task of promulgating regulations be left with the secretary of state or other central authority?

4. Section 504 requires regulating authorities to take account of consistency in applications and interoperability to the extent practicable when promulgating regulation. This section is critical in addressing the concerns of many at our meetings that inconsistent applications may promote barriers greater than currently exist.

PART 6

MISCELLANEOUS PROVISIONS

SECTION 601. SEVERABILITY CLAUSE. If any provision of this [Act] or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this [Act] which can be given effect without the invalid provision or application, and to this end the provisions of this [Act] are severable.

Source: Article 1 Draft Section 1-106.

SECTION 602. EFFECTIVE DATE. This [Act] takes effect .....

Source:

SECTION 603. SAVINGS AND TRANSITIONAL PROVISIONS.

Source: