

DRAFT

FOR DISCUSSION ONLY

UNIFORM ELECTRONIC TRANSACTIONS ACT

NATIONAL CONFERENCE OF COMMISSIONERS

ON UNIFORM STATE LAWS

MARCH 23, 1998

UNIFORM ELECTRONIC TRANSACTIONS ACT

With Comments

COPYRIGHT© 1998

by

NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS

The ideas and conclusions herein set forth, including drafts of proposed legislation, have not been passed on by the National Conference of Commissioners on Uniform State Laws. They do not necessarily reflect the views of the Committee, Reporters or Commissioners. Proposed statutory language, if any, may not be used to ascertain legislative meaning of any promulgated final law.

**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 Street, 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 Dr., Lakeland, FL 33802-2092, Division Chair

AMERICAN BAR ASSOCIATION ADVISORS

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

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

1 UNIFORM ELECTRONIC TRANSACTIONS ACT

2 TABLE OF CONTENTS

3 PART 1

4 GENERAL PROVISIONS

5 SECTION 101. SHORT TITLE.

6 SECTION 102. DEFINITIONS.

7 SECTION 103. SCOPE.

8 SECTION 104. TRANSACTIONS SUBJECT TO OTHER LAW.

9 SECTION 105. VARIATION BY AGREEMENT.

10 SECTION 106. APPLICATION AND CONSTRUCTION.

11 ~~SECTION 107. COURSE OF PERFORMANCE, COURSE OF DEALING, AND USAGE~~
12 ~~OF TRADE.~~

13 ~~[SECTION 1078. MANIFESTING ASSENT.]~~

14 ~~[SECTION 1089. OPPORTUNITY TO REVIEW.]~~

15 ~~SECTION 10910. DETERMINATION OF COMMERCIALLY REASONABLE SECURITY~~
16 ~~PROCEDURE; COMMERCIALLY UNREASONABLE SECURITY~~
17 ~~PROCEDURE; NO SECURITY PROCEDURE.~~

18 ~~SECTION 110. EFFECT OF REQUIRING A COMMERCIALLY UNREASONABLE~~
19 ~~SECURITY PROCEDURE.~~

20 ~~SECTION 111. OBLIGATION OF GOOD FAITH.~~

21 ~~SECTION 112. GENERAL PRINCIPLES OF LAW APPLICABLE.~~

22 PART 2

23 ELECTRONIC RECORDS GENERALLY

24 SECTION 201. LEGAL RECOGNITION OF ELECTRONIC RECORDS.

25 SECTION 202. ATTRIBUTION OF ELECTRONIC RECORD TO A PERSON PARTY.

26 SECTION 203. DETECTION OF CHANGES AND ERRORS.

27 SECTION 204. ORIGINALS - INFORMATION ACCURACY.

28 SECTION 205. RETENTION OF ELECTRONIC RECORDS.

29 PART 3

30 ELECTRONIC SIGNATURES GENERALLY

31 SECTION 301. LEGAL RECOGNITION OF ELECTRONIC SIGNATURES.

32 SECTION 302. ELECTRONIC SIGNATURES EFFECT AND PROOF.

33 SECTION 303. ~~{SIGNATURES BY}~~ ~~{OPERATIONS OF}~~ ELECTRONIC AGENTS.

1 PART 4
2 ELECTRONIC CONTRACTS AND COMMUNICATIONS

3 SECTION 401. FORMATION AND VALIDITY.
4 SECTION 402. TIME AND PLACE OF SENDING AND RECEIPT.
5 SECTION 403. ELECTRONIC ACKNOWLEDGMENT OF RECEIPT.
6 SECTION 404. ADMISSIBILITY INTO EVIDENCE.
7 SECTION 405. TRANSFERABLE RECORDS.

8 PART 5
9 GOVERNMENTAL ELECTRONIC RECORDS

10 SECTION 501. USE CREATION AND RETENTION OF ELECTRONIC RECORDS
11 AND CONVERSION OF WRITTEN RECORDS BY STATE
12 GOVERNMENTAL AGENCIES.
13 SECTION 502. RECEIPT AND DISTRIBUTION OF ELECTRONIC RECORDS BY
14 GOVERNMENTAL AGENCIES.
15 SECTION 503. [DESIGNATED STATE OFFICER] TO ADOPT STATE
16 STANDARDS.
17 SECTION 504. INTEROPERABILITY.

18 PART 6
19 MISCELLANEOUS PROVISIONS

20 SECTION 601. SEVERABILITY.
21 SECTION 602. EFFECTIVE DATE.
22 SECTION 603. SAVINGS AND TRANSITIONAL PROVISIONS.

1
2
3
4
5
6
7
8
9
0
1
2
3
4
5
6
7
8
9
0
1
2
3
4
5
6
7
8

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

(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, ~~including course of performance, course of dealing and usage of trade as provided in this [Act].~~ Whether an agreement has legal consequences is determined by this [Act], if applicable, ~~or~~⁷ otherwise by other applicable rules of law.

Source: Revised Article 1, Section 1-201(3) (Sept. 1997 Draft)

Textual References: Section 105. Variation by Agreement; Section 202. Attribution of Electronic Record; Section 401. Formation and Validity.

Committee Votes:

1. To delete the concept of manifestation of assent from the definition - By consensus (no formal vote) (Sept. 1997)
2. To delete course of performance, course of dealing and usage of trade: Committee 4 Yes - 2 No; Observers 6 Yes - 1 No. (Jan. 1998)

Notes to This Draft: 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

1 law outside this Act. In light of this principle the prior
2 references to usage evidence as informing the content of an
3 agreement was considered substantive, and therefore, best left to
4 other law outside this Act.

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

11 **Reporter's Note:** Whether the parties have reached an agreement
12 is determined by their express language and surrounding
13 circumstances. The Restatement of Contracts §3 provides that

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

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

22 The existence and content of an agreement under this Act is
23 determined by the parties' language and surrounding
24 circumstances. The relevant surrounding circumstances and the
25 context of the transaction will inform the precise terms of any
26 agreement. The second sentence of this definition makes clear
27 that the substantive law applicable to an electronic transaction
28 effectuated by this Act must be applied to determine those
29 circumstances relevant in establishing the precise scope and
30 meaning of the parties' agreement.

31 The comment to this definition will make clear that, though
32 derived from the UCC definition, there is no intent to affect the
33 meaning of the term under the UCC or any other applicable law.
34

35 (2) "Automated transaction" means a ~~commercial or~~
36 ~~governmental~~ transaction formed or performed, in whole or in
37 part, by electronic means or electronic records in which the acts
38 or records of one or both parties ~~will~~ are not ~~be~~ reviewed by an
39 individual as an ordinary step in forming a contract, performing
40 under an existing contract, or fulfilling any obligation required
41 by the transaction.

42 **Source:** Article 2B Draft Section 2B-102(a)(4)

43 **Textual References:** Section 204. Inadvertent Error; Section 401.
44 Formation and Validity.

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

4 **Notes to This Draft:** Edited to reflect Committee vote and to
5 more closely track Article B.

6 **Reporter's Note:** Article 2B has conformed its terminology with
7 this Act by adopting "automated transaction" in place of
8 "electronic transaction." The definitions in each are
9 conceptually the same. The definition in this Act is broader,
10 going beyond contract formation to performances under a contract
11 and other obligations accomplished by electronic agents in a
12 transaction, because of the diversity of transactions to which
13 this Act may apply.

14 As with electronic agents, this definition addresses the
15 circumstance where electronic records may result in action or
16 performance by a party although no human review of the electronic
17 records is anticipated. Section 401(b) provides specific
18 contract formation rules where one or both parties do not review
19 the electronic records.
20

21 ~~(3) "Commercial transaction" means all matters arising~~
22 ~~in a commercial setting, whether contractual or not including,~~
23 ~~but not limited to, the following: any trade transaction for the~~
24 ~~supply or exchange of goods, information or services;~~
25 ~~distribution agreements; commercial representation or agency;~~
26 ~~factoring; leasing; construction of works; consulting;~~
27 ~~engineering; licensing; investment; financing; banking;~~
28 ~~insurance; exploitation agreement or concession; joint venture~~
29 ~~and other forms of industrial or business cooperation or~~
30 ~~organization; carriage of goods or passengers by air, sea, rail~~
31 ~~or road.~~

32 **Committee Vote:** To delete definition: Committee 4 Yes (Chair
33 broke tie) - 3 No; Observers 19 Yes - 1 No. (Jan. 1998)

34 **Reporter's Note:** This definition was deleted as too broad, and
35 unnecessary in light of the approach to Scope and exclusions
36 adopted by the Committee at the January, 1998 meeting. See
37 Reporter's Notes to Sections 103 and 104 below.

(34) "Computer program" means a set of statements or instructions to be used directly or indirectly ~~to operate in~~ an information processing system in order to bring about a certain result. The term does not include informational content ~~created or communicated as a result of the operation of the system.~~

Source: Article 2B Draft Section 2B-102(a)(6).

Textual References: Section 102. "Electronic Agent," "Information". Section 202. Attribution of Electronic Record.

Notes to This Draft: Edited for clarity and to more closely track Article 2B.

Reporter's Note: This definition is from Article 2B. The term is used principally with respect to the definition of "electronic agent" and "information." Is it a necessary definition? Is it an accurate definition?

(45) "Contract" means the total legal obligation ~~which results~~ resulting from the parties' agreement as affected by this [Act] and ~~as supplemented by~~ other applicable rules of law.

Source: UCC Section 1-201(11)

Textual References: Section 401. Formation and Validity.

(56) "Electronic" means electrical, digital, magnetic, wireless, optical, or electromagnetic technology, or any other ~~form of technology that entails similar capabilities similar to these technologies.~~

Source: Article 2B Draft Section 2B-102(17).

Textual References: Section 102. "Electronic agent," "Electronic record," "Electronic signature," "Record". Section 105. Variation by Agreement. Section 401. Formation and Validity. Section 403. Electronic Acknowledgement of Receipt.

Notes to This Draft: This definition has been edited to more closely track Article 2B. The "of or relating to" language in Article 2B is unnecessary and creates potential ambiguity.

Reporter's Note: 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. Query whether the definition is broad enough?

(67) "Electronic agent" means a computer program or other electronic or automated means used, selected, or programmed by a person to initiate or respond to electronic records or performances in whole or in part without review by an individual.

Source: Article 2B Draft Section 2B-102(a)(18).

Textual References: Section 102. "Electronic Signature," "Signature". Section 107. Manifesting Assent. Section 108. Opportunity to Review. Section 202. Attribution of Electronic Record. Section 204. Inadvertent Error. Section 302. Electronic Signatures: Effect and Proof. Section 303. Operations of Electronic Agents. Section 401. Formation and Validity.

Reporter's Note: An electronic agent, as a computer program or other automated device 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 agent by definition is capable, within the parameters of its programming, of initiating, responding or interacting with other parties or their electronic agents 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 agents in the absence of human intervention.

While this Act proceeds on the paradigm that an electronic agent 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 agents 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). At such time as this may occur, "Courts may ultimately conclude that an electronic agent is equivalent in all respects to a human agent..." Article 2B-102, Reporter's Note 10.

Section 303 and Section 401 make clear that the party that sets operations of an electronic agent 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.

(78) "Electronic record" means a record created, stored, generated, received, or communicated by electronic

1 means, ~~such as information systems, computer equipment and~~
2 ~~programs, electronic data interchange, electronic mail, or voice~~
3 ~~mail, facsimile, telex, telecopying, scanning, and similar~~
4 ~~technologies.~~

5 **Source:** Article 2B Draft Section 2B-102(a)(19)

6 **Textual References:** Passim.

7 **Notes to this Draft:** The last clause has been deleted and moved
8 to the comment to avoid confusion. Comments to the prior draft
9 suggested that these means of accomplishing an electronic record,
10 were themselves electronic records. The list of mechanisms has
11 been included in the comment/note below.

12 **Reporter's Note:** An electronic record is a subset of the broader
13 defined term "record." Unlike the term "electronic message" used
14 in Article 2B, the definition is not limited to records intended
15 for communication, but extends to any information contained or
16 transferred in an electronic medium. It is also used in this Act
17 as a limiting definition in those provisions in which it is used.

18 Electronic means for creating, storing, generating,
19 receiving or communicating electronic records include information
20 processing systems, computer equipment and programs, electronic
21 data interchange, electronic mail, or voice mail, facsimile,
22 telex, telecopying, scanning, and similar technologies.

23
24 (89) "Electronic signature" means any signature in
25 electronic form, attached to or logically associated with an
26 electronic record, ~~executed or adopted by a person or its~~
27 ~~electronic agent with intent to sign the electronic record.~~

28 **Source:** UCC Section 1-201(39); Illinois Model Section 200(3).

29 **Textual References:** Passim.

30 **Notes to This Draft:** The last clause has been deleted as
31 redundant of the definition of signature.

32 **Reporter's Note:** As with electronic record, this definition is a
33 subset of the broader defined term "signature." The purpose of
34 the separate definition is principally one of clarity in
35 extending the definition of signature to the electronic
36 environment.

37 This definition has been simplified by using the defined
38 term "signature" within this definition. The defined term
39 "signature" has been expanded from the standard UCC definition to
40 incorporate specifically the attributes normally attached to a
41 written signature, and to track the concept of authentication as
42 defined in Article 2B. The new definition of "signature"
43 reflects the Committee's direction to delete the term

1 "authenticate" from the August Draft and incorporate that
2 definition into "signature."

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

14 An electronic signature includes any symbol adopted by a
15 party, so long as the requisite intent to authenticate the
16 electronic record exists (See definition of Signature). There is
17 no requirement that there be "present intent" to sign because of
18 the potential barrier to the efficacy of electronic signatures.
19 While a contemporaneous signature would reflect a present intent
20 to sign, the operations of an electronic agent which result in
21 the creation of an electronic signature (See Section 303) may not
22 be viewed by courts as manifesting a "present" intent since the
23 act of programming the electronic agent may have occurred well
24 before the attachment of the electronic signature.

25 A digital signature using public key encryption technology
26 would qualify as an electronic signature, as would the mere
27 appellation of one's name at the end of an e-mail message - so
28 long as in each case the signature was applied with the intention
29 to authenticate the electronic record with which it was
30 associated. It is the adoption of the symbol with intention to
31 authenticate that is controlling. See *Parma Tile Mosaic & Marble*
32 *Co. v. Estate of Short*, 87 NY2d 524 (1996) where it was held that
33 the automatic imprint of a firm name, programmed into a fax
34 machine, was not a sufficient signature because of the absence of
35 any intention to authenticate each document sent over the fax.
36

37 ~~(10) "Good faith" means honesty in fact and the~~
38 ~~observance of reasonable commercial standards of fair dealing.~~

39 **Source:** Revised Article 1 Section 1-201(22) (Sept. 1997 draft)

40 **Committee Vote:** To delete Section 111 Obligation of Good Faith -
41 Committee 6 Yes - 1 No; Observers 7 Yes - 5 No. (Jan. 1998)

42 **Notes to This Draft:** The definition and obligation of good faith
43 (former Section 111) have been deleted. The Committee's view was
44 that the obligation of good faith was an issue to be determined
45 as a matter of the substantive law applicable to the underlying
46 transaction. Accordingly, the issue of whether good faith is
47 required, and its impact on a given transaction is left to the
48 substantive law applicable to the particular transaction outside
49 this Act.

(922) "State Governmental agency" means any 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.

Source: New.

Textual References: Section 104. Excluded Transactions. Part 5. Passim.

Notes to This Draft: This is the definition of "State agency" from the former Draft. It has been revised to be more appropriately descriptive of agencies at the local and county levels included within the definition.

Reporter's Note: 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 in light of comment from members of the Committee that these should not be included. The Reporter seeks direction from the Committee on whether the legislative and judicial branches should be excluded.

~~(11) "Governmental transaction" means all matters arising in any governmental setting, including, but not limited to, the following: all communications, filings, reports, commercial documentation, or other electronic records relating to interactions between any governmental entity and any individual outside the government; and all intragovernmental communications, documents or other records employed in the conduct of governmental functions between or within any branch or agency of government.~~

Committee Vote: To delete definition and reference in section on Scope: Committee 4 Yes - 3 No (Chair broke tie); Observers 19 Yes - 1 No.

Reporter's Note: This definition was deleted in light of the Committee's approach to Scope. See Reporter's Notes to Section 103. Scope.

(1012) "Information" means data, text, images, sounds, codes, computer programs, software, databases, ~~and~~ or the like.

Source: Illinois Model Section 200(4); Article 2B Draft Section 2B-102(a) (23).

Textual References: Section 102. "Informational content," "Information processing system," "Notify," "Record". Section 107. Manifestation of Assent. Section 110. Effect of Requiring Commercially Unreasonable Security Procedure. Section 205. Originals: Accuracy of Information. Section 206. Retention of

Electronic Records. Section 402. Time and Place of Sending and Receipt.

(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.

Source: Article 2B Draft Section 2B-102(25).

Textual References: Section 102. "Security procedure". Section 203. Detection of Changes and Errors. Section 302. Electronic Signatures:Effect and Proof.

Reporter's Note: 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. The example from Article 2B most clearly 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.

(1213) "Information processing system" means a system for creating, generating, sending, receiving, storing, displaying, or otherwise processing information, including electronic records.

Source: Uncitral Model Article 2(f); Article 2B Draft Section 2B-102(a) (24).

Textual References: Section 402. Time and Place of Sending and Receipt.

Reporter's Note: 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. Query the accuracy and completeness of this definition?

(1314) "Notify" means to communicate, or make available, information to another person in a form and manner as appropriate or required under the circumstances.

Source: Illinois Model Section 103(22) (June 4 Interim Draft).

Textual References: Section 203. Detection of Changes and Errors. Section 403. Electronic Acknowledgement of Receipt.

Reporter's Note: 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.

~~(1415) "Organization" means a person other than an individual.~~

Source: UCC Section 1-201(28).

Textual References: None.

Reporter's Note: Although, this is a standard Conference definition, it has been deleted since it is not used.

~~(1416) "Person" means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, government, governmental subdivision, or agency, or instrumentality, or public corporation, or any other legal or commercial entity.~~

Source: CC Section 1-201(30).

Textual References: Passim

Reporter's Note: This is the standard Conference formulation for this definition.

[ALTERNATIVE 1]

~~(1517) "Presumption" or "presumed" means that the trier of fact must find the existence of the fact presumed unless and until evidence is introduced which would support a finding of its non-existence.~~

Source: UCC Section 1-201(31)

[ALTERNATIVE 2]

~~(1517) "Presumption" means that when a fact or group of facts giving rise to a presumption (the "basic fact") exists, the existence of the fact to be assumed upon a finding of the~~

1 basic fact (the "presumed fact") must be assumed unless and until
2 the party against whom the presumption is directed produces
3 evidence which would support a finding of the non-existence of
4 the presumed fact. "Presumed" has a corresponding meaning.

5 **Source:** Derived from the definitions in Revised Uniform Rules
6 of Evidence 301 and 302

7 [ALTERNATIVE 3]
8 (1517) "Presumption" means an inference of fact in
9 issue which the law requires to be drawn from certain proven
10 facts, unless and until the party against which the inference is
11 directed produces evidence which would support a finding of its
12 non-existence. "Presumed" has a corresponding meaning.

13 **Source:**___Derived from revision suggested by Committee on Style.

14 **Textual References:** Section 110. Effect of Requiring Commercially
15 Unreasonable Security Procedure. Section 202. Attribution of
16 Electronic Record. Section 203. Detection of Changes and
17 Errors. Section 302. Electronic Signatures:Effect and Proof.
18 Section 403. Electronic Acknowledgement of Receipt.

19 **Reporter's Note:** This definition is necessary to indicate the
20 effect of the presumptions created by Sections 202, 203 and 302.
21 While the decision whether a presumption should be created is
22 generally one of policy relating to the substantive law, the
23 effect to be given to a presumption once created is generally
24 left to the rules of evidence. THE QUESTION FOR THE COMMITTEE is
25 whether this Act should address the effect of a presumption
26 created by this Act.

27 Each of the above alternatives adopts the so-called
28 "bursting bubble" approach to presumptions. That is, only the
29 burden of producing evidence shifts, but not the ultimate burden
30 of persuasion. Alternative 1 reflects the current definition in
31 the UCC. The Reporter was advised by Neil Cohen, Reporter for
32 the revision of Article 1, that the committee has taken a strong
33 position that the definition should not be changed.

34 Alternative 2 is derived from the most recent draft of Rules
35 301 and 302 of the Revised Uniform Rules of Evidence which the
36 Reporter has seen. The draft of Rule 302 currently provides:

37 In all civil actions and proceedings not otherwise provided
38 for by statute, by judicial decision, or by these rules, a
39 presumption imposes on the party against whom it is directed

1 the burden of proving that the nonexistence of the presumed
2 fact is more probable than its existence.

3 This provision goes beyond the "bursting bubble" approach and
4 shifts the ultimate burden of persuasion regarding the presumed
5 fact.

6 Alternative 3 is based on the revision suggested by the
7 Committee on Style. The Committee on Style's revision provides:

8 "Presumption" means an inference of fact in issue which the
9 law requires to be drawn from certain known facts and which
10 substitutes for evidence of the presumed fact unless the
11 party against which it is directed proves that its
12 nonexistence is more probable than its existence. "Presumed"
13 has a corresponding meaning.

14 The effect of this definition also would result in the shifting
15 of the burden of persuasion. In addition, while a presumption
16 may be viewed as a legally required inference, it is not
17 considered to be a substitute for evidence of the presumed fact.
18 2 McCormick on Evidence, §344 (Strong ed., 4th ed. 1992); Mueller
19 and Kirkpatrick, Evidence §3.8 (Little Brown, 1995).

20 All alternatives in this draft have been revised, when
21 necessary, to provide for the lesser effect of a "bursting
22 bubble" presumption.

23 This draft creates presumptions, in those circumstances
24 where the parties have agreed to or adopted a security procedure
25 which is commercially reasonable, regarding 1) attribution of an
26 electronic record to a party (202(b)); the absence of changes
27 (203(a)) and errors (203(b)) in an electronic record; and the
28 existence, authenticity and authority to make an electronic
29 signature (302(b)). Under Section 105(a) the parties remain free
30 to alter the effect to be given to electronic records and
31 signatures affected by the use of security procedures, i.e., the
32 parties may agree to stronger or weaker presumptions which may
33 attach.

34 The effect of a bursting bubble presumption is demonstrated
35 by McCormick in reference to the presumption of receipt of a
36 properly addressed and posted letter. McCormick notes:

37 [T]he defendant may destroy the presumption by denying
38 receipt. Nevertheless, a jury question is presented, not
39 because of the presumption, but because of the natural
40 inference flowing from the plaintiff's showing that she had
41 mailed a properly addressed letter that was not returned.

42 2 McCormick on Evidence §344. Similarly, when a party proves the
43 implementation of a commercially reasonable security procedure,
44 the other party may destroy the presumption (e.g., attribution,
45 lack of errors, etc.), by directly denying the presumed fact
46 (attribution, error, etc). However, a jury question may remain
47 based on the strength of the evidence of the security procedure

1 and the natural inference that, if followed the security
2 procedure would demonstrate that the electronic record was that
3 of the sender, did not contain errors, etc.

4 This "soft presumption" is appropriate in this Act given the
5 uncertainties in the development and robustness of security
6 procedures. It places on the party against whom the presumption
7 is directed the obligation to expressly and directly deny the
8 fact of attribution, lack of error, etc. At the same time, the
9 proof regarding the quality of the security procedure gives rise
10 to an inference (stronger or weaker, depending on the quality of
11 the procedure) that the existence of the presumed fact is more
12 credible than the party's denial.

13 (1618) "Record" means information that is inscribed on
14 a tangible medium or that is stored in an electronic or other
15 medium and is retrievable in perceivable form.

16 **Source:** Article 2B Draft Section 2B-102(a) (37).

17 **Textual References:** Section 102. "Automated Transaction,"
18 "Electronic Record," "Signature," "Transferable Record,"
19 "Writing". Section 105. Variation by Agreement. Section 107.
20 Manifestation of Assent. Section 108. Opportunity to Review.
21 Section 201. Legal Recognition of Electronic Records. Section
22 203. Detection of Changes and Errors. Section 205.
23 Originals:Accuracy of Information. Section 206. Retention of
24 Electronic Records. Section 302. Electronic Signatures:Effect
25 and Proof. Section 401. Formation and Validity. Section 403.
26 Electronic Acknowledgement of Receipt. Section 405. Transferable
27 Records. Section 501. Creation and Retention of Records...

28 **Reporter's Note:** This is the standard Conference formulation for
29 this definition.

30 (1719) "Rule of law" means a statute, regulation,
31 ordinance, common-law rule, court decision, or other law ~~relating~~
32 ~~to commercial or governmental transactions~~ enacted, established,
33 or promulgated by in this State, or any agency, commission,
34 department, court, or other authority or political subdivision of
35 this State.

36 **Source:** Oklahoma Model Section II.F; Illinois Model Section
37 200(7).

38 **Textual References:** Section 201. Legal Recognition of Electronic
39 Records. Section 205. Originals:Accuracy of Information.
40 Section 206. Retention of Electronic Records. Section 301. Legal
41 Recognition of Electronic Signatures.

1 **Reporter's Note:** The definition is drafted broadly. The former
2 limitation relating to commercial and governmental transactions,
3 has been deleted in light of the Committee's vote regarding the
4 manner of defining the Scope of this Act.

5 (1820) ~~"Security procedure," with respect to either an~~
6 ~~electronic record or electronic signature, means a commercially~~
7 ~~reasonable procedure or methodology, established by law or~~
8 ~~regulation, or established by agreement, or adopted by the~~
9 ~~parties, for the purpose of verifying that an electronic~~
10 ~~signature, record, or performance is that of a specific person or~~
11 ~~for detecting changes or errors in the informational content of~~
12 ~~an electronic record. (i) the identity of the sender, or source,~~
13 ~~of an electronic record, or (ii) the integrity of, or detecting~~
14 ~~errors in, the transmission or informational content of an~~
15 ~~electronic record. A security~~ The term includes a procedure ~~may~~
16 that requires the use of algorithms or other codes, identifying
17 words or numbers, encryption, callback or other acknowledgment
18 procedures, or any other procedures that are reasonable under the
19 circumstances.

20 **Source:** Article 2B Draft Section 2B-102(a)(2); Illinois Model
21 Section 200(9); UCC Section 4A-201; Oklahoma Model Section
22 III.B.2.

23 **Textual References:** Section 105. Variation by Agreement.
24 Section 109. Determination of Commercially Unreasonable Security
25 Procedure. Section 110. Effect of Requiring a Commercially
26 Unreasonable Security Procedure. Section 202. Attribution of
27 Electronic Records. Section 203. Detection of Changes and
28 Errors. Section 302. Electronic Signatures:Effect and Proof.
29 Section 302.

30 **Notes to This Draft:** Edited for clarity and to more closely
31 track Article 2B definition of "attribution procedure," and also
32 to eliminate the requirement that, as defined, a security
33 procedure must be commercially reasonable. The element of
34 commercial reasonableness remains important in the determination
35 of the applicability of presumptions which may attach to the use
36 of security procedures in Sections 202, 203 and 302.

Reporter's Note: Limiting security procedures to those which are either agreed to or adopted by parties or established by law or regulation, together with the requirement that only commercially reasonable security procedures give rise to limited presumptions, eliminates much of the concern over the creation of the limited presumptions in Sections 202, 203 and 302. 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 have been expanded in this draft to 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.

(19) "Sign" means the to executeion or adoption of a signature by a person or the person's electronic agent.

Source: UETA Section 102(21) (Nov. 25, 1997 Draft)

Textual References: Section 107. Manifestation of Assent. Section 302. Electronic Signatures:Effect and Proof. Section 303. Operations of Electronic Agents. Section 404. Admissibility Into Evidence. Section 502. Receipt and Distribution of Electronic Records...

Reporter's Note: This definition has been moved from the end of the definition of signature in the prior draft and revised to conform to style committee comments.

(20~~1~~) "Signature" means any symbol, sound, process, or encryption of a record in whole or in part, executed or adopted by a person or the person's electronic agent with intent to:

(i~~A~~) identify the party that person;

(i~~i~~B) adopt or accept a term or a record; or

(i~~ii~~C) establish the informational integrity of a record or term that contains the signature or to which a record containing the signature refers.

~~"Sign" means the execution or adoption of a
signature by a person or the person's electronic agent.~~

Source: UCC Section 1-201(39); Article 2B Draft Section 2B-102(a) (3)

Textual References: Section 102. "Electronic signature," "Sign".
Section 105. Variation by Agreement. Section 301. Legal
Recognition of Electronic Signatures.

Notes to This Draft: Edited for clarity.

Reporter's Note: 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 prior definition of authenticate have been carried into this definition of signature.

[~~(2123)~~ "Term" means that portion of an agreement
which relates to a particular matter.]

Source: UCC Section 1-201(42)

Textual References: Section 102. "Signature." Section 107.
Manifesting Assent. Section 108. Opportunity to Review. Section
202. Attribution of a Record. Section 302. Electronic
Signatures:Effect and Proof. Section 401. Formation and
Validity.

Reporter's Note: 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.

(~~2224~~) "Transferable record" means a record, other
than a writing, that ~~is~~ 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.

Source: Oklahoma Model Section II.H.

Textual References: Section 405. Transferable Records.

Reporter's Note: This definition is necessary in the event the Drafting Committee decides to retain the applicability of this Act to such records. See Section 405.

(2325) "Writing" includes printing, typewriting, ~~or~~ and any other intentional reduction of a record to tangible form. "Written" has a corresponding meaning.

Source: UCC Section 1-201(46).

Textual References: Section 102. "Transferable record." Section 201. Legal Recognition of Electronic Records. Section 206. Retention of Electronic Records. Section 501. Creation and Retention...

Reporter's Note: This definition reflects the current UCC definition.

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

"Basic fact". Section 102(15)

"Inadvertent error". Section 204

"Presumed fact". Section 102(15)

"Relying person". Section 202

"Requiring party". Section 110

"Responsible person". Section 202

Source: UCC Section 2-103(b).

SECTION 103. SCOPE. (a) Except as otherwise provided in Section 104 ~~or any regulation adopted pursuant to Part 5,~~ this [Act] applies to electronic records and electronic signatures generated, stored, processed, communicated, or used for any purpose in any ~~commercial or governmental~~ transaction.

(b) Principles of law and equity shall be used to supplement this [Act] except to the extent that those principles are

1 [inconsistent with] [displaced by] the terms[, purposes and
2 policies] of a particular provision of this [Act].

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

5 **Committee Votes:**

6 1. To delete references to commercial and governmental
7 transactions - Committee 4 Yes - 3 No (Chair broke tie) Observers
8 19 Yes - 1 No.

9 2. To incorporate supplemental principles as part of Scope
10 section - Committee Yes Unanimous Observers 12 Yes - 0 No

11 **Notes for This Draft:** The Scope section has been edited to
12 reflect the Committee's view that this Act should apply to all
13 transactions in which electronic records and signatures are used,
14 unless specifically excluded under the next Section.

15 **Reporter's Note:**

16 1. The scope of the Act has been clarified by limiting its
17 applicability to electronic records and adding electronic
18 signatures. The underlying premise of this section is that this
19 Act applies to all electronic records and signatures unless
20 specifically excluded by the next Section.

21 2. Notwithstanding the apparent simplicity and clarity of this
22 revised section, the Scope of this Act remains one of the most
23 difficult aspects in the drafting of this Act. At the January
24 meeting it was the view of many observers and members of the
25 Committee, that the attempt to limit scope based on the
26 definition of commercial and governmental transactions was
27 unworkably vague, while at the same time being overly broad (one
28 committee member noted that under the prior draft a secretary in
29 a bank getting a cup of coffee would be covered). In order to
30 achieve clarity and precision, the committee narrowly voted to
31 eliminate the restriction to commercial and governmental
32 transactions. The approach now being taken is to delineate with
33 specificity, in the next section, those transactions and types of
34 transactions which will be excluded.

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

44 At the May, 1997 meeting, the Drafting Committee expressed
45 strong reservations about applying this Act to all writings and
46 signatures, as is contemplated in the Illinois, Massachusetts and
47 other models. These same reservations were again raised at the
48 September Meeting. The scope section appearing in the last draft

1 was an attempt to address those concerns by limiting
2 applicability of the Act to only those records and signatures
3 arising in the context of a commercial or governmental
4 transaction, as therein defined. However, the view of a majority
5 of the committee and most observers was that a specific
6 delineation of excluded transactions in the next section was
7 preferable to the attempt to redefine commercial and governmental
8 transactions.

9 6. Section 104 will set forth specific exclusions to the
10 coverage of this Act based on the work of the Task Force. As of
11 the finalization of this Draft, however, that work was still in
12 progress. It is hoped that some delineation will be available by
13 the time of the April 17 meeting. Exclusions from the coverage
14 of this Act will be set forth in a single section.

15 **SECTION 104. EXCLUDED TRANSACTIONS ~~SUBJECT TO OTHER LAW.~~**

16 ~~(a) This [Act] does not apply to the extent that its~~
17 ~~application would involve a construction of a rule of law that is~~
18 ~~clearly inconsistent with the manifest intent of the lawmaking~~
19 ~~body or repugnant to the context of the same rule of law,~~
20 ~~provided that the mere requirement that information be "in~~
21 ~~writing," "written," "printed," "signed," or any other word that~~
22 ~~specifies or requires the use of a particular medium of~~
23 ~~presentation, communication or storage, shall not, by itself, be~~
24 ~~sufficient to establish such intent.~~

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

26 ~~(1) any applicable rules of law relating to consumer~~
27 ~~protection;~~

28 ~~(2) the Uniform Commercial Code as enacted in this~~
29 ~~State; and~~

30 ~~(3) [OTHER]{such other rules of law as may be~~
31 ~~designated at the time of the enactment of this [Act]}.~~

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

6 (a) This [Act] does not apply to the following
7 transactions:

8 (1) Transactions governed by the Uniform Commercial
9 Code as enacted in this state, except to the extent provided in
10 Section 405;

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

13 (3) Transactions specifically excluded by any
14 governmental agency pursuant to Part 5 of this [Act].

15 (b) This [Act] does not apply to any transaction which is
16 subject to legislation enacted after the effective date of this
17 [Act] which expressly provides that this [Act] shall not apply.

18 **Source:** New

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

23 **Notes to This Draft:** This section has been revised to reflect
24 the Committee's position that, unless excluded, this Act will
25 apply to all electronic records and signatures used in any
26 transaction.

27 **Reporter's Note:**

28 1. The prior draft reflected comments made at the September,
29 1997 meeting.

30 2. The "repugnancy clause" set forth in the prior draft was
31 similar to those appearing in the Mass. and Ill. Acts. The view
32 that such a clause was too ambiguous and impossible to apply was
33 widely shared among both the observers and members of the

Committee. Accordingly, it has been deleted, notwithstanding the view among a few observers and members of the Committee that such a safeguard remains necessary.

3. 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 meeting to review statutory compilations in order to identify candidates for exclusion.

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 the provisions of this [Act] may be varied by agreement, ~~except:~~

(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.

~~(1) the obligations of good faith, reasonableness, diligence and care prescribed by this [Act] may not be disclaimed by agreement but the parties may by agreement determine the standards by which the performance of such obligations is to be measured if such standards are not manifestly unreasonable; and~~

~~(2) the rules in Section 110 regarding allocations of loss where no security procedure or commercially unreasonable security procedures are used in a transaction.~~

~~(d)~~ The presence in certain provisions of this [Act] of the words "unless otherwise agreed" or words of similar import or

1 does not imply that the effect of other provisions may not be
2 varied by agreement under subsection (a).

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

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

7 **Reporter's Note:**

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

17 The only provisions of the Act which may not be disclaimed
18 by agreement are those establishing the method and manner of
19 determining the commercial reasonableness of a security
20 procedure, and determining the effect of requiring the use of a
21 commercially unreasonable security procedure. **QUESTION FOR THE**
22 **COMMITTEE: Are there other provisions of this Act which should be**
23 **mandatory?**

24 2. Subsection (e) makes clear that this Act is intended to
25 permit the use of electronic media, but does not require any
26 person to use electronic media. For example, if Chrysler Corp.
27 were to issue a recall of automobiles via its internet website,
28 it would not be able to rely on this Act to validate that notice
29 in the case of a person who never logged on to the website, or
30 indeed, had no ability to do so. The provisions in Sections
31 201(c) and 301(c) permitting a person to establish reasonable
32 forms for electronic records and signatures assumes a pre-
33 existing relationship between parties to a transaction, in which
34 one party places reasonable limits on the records and signatures,
35 electronic or otherwise, which will be acceptable to it.
36

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

41 **Source:** UCC Section 1-102

1 **Committee Vote:** To delete the word underlying Committee 2 Yes -1
2 No Observers 14 Yes - 2 No

3 **Reporter's Note:** The following commentary, derived from the
4 Illinois Electronic Commerce Security Act Section 102, has been
5 moved from the text of former Section 103 in the August Draft.

6 The purposes and policies of this Act are

7 a) to facilitate and promote commerce and governmental
8 transactions by validating and authorizing the use of electronic
9 records and electronic signatures;

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

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

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

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

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

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

29 ~~**SECTION 107. COURSE OF PERFORMANCE, COURSE OF DEALING, AND**~~
30 ~~**USAGE OF TRADE.**~~

31 ~~(a) A course of performance is a sequence of conduct~~
32 ~~between the parties to a particular transaction which exists if:~~

33 ~~(1) the agreement of the parties with respect to~~
34 ~~the transaction involves repeated occasions for performance by a~~
35 ~~party;~~

36 ~~(2) that party performs on one or more occasions;~~
37 ~~and~~

1 ~~(3) the other party, with knowledge of the nature~~
2 ~~of the performance and opportunity for objection to it, accepts~~
3 ~~the performance or acquiesces to it without objection.~~

4 ~~(b) A course of dealing is a sequence of previous~~
5 ~~conduct between the parties to a particular transaction which is~~
6 ~~fairly to be regarded as establishing a common basis of~~
7 ~~understanding for interpreting their expressions and other~~
8 ~~conduct.~~

9 ~~(c) A usage of trade is any practice or method of~~
10 ~~dealing having such regularity of observance in a place,~~
11 ~~vocation, or trade as to justify an expectation that it will be~~
12 ~~observed with respect to the transaction in question. The~~
13 ~~existence and scope of the usage are to be proved as facts. If~~
14 ~~it is established that the usage is embodied in a trade code or~~
15 ~~similar record, the interpretation of the record is a question of~~
16 ~~law.~~

17 ~~(d) A course of performance or course of dealing~~
18 ~~between the parties or usage of trade in the vocation or trade in~~
19 ~~which they are engaged or of which they are or should be aware is~~
20 ~~relevant in ascertaining the meaning of the parties' agreement,~~
21 ~~may give particular meaning to specific terms of the agreement,~~
22 ~~and may supplement or qualify the terms of the agreement. A~~
23 ~~usage of trade applicable where only part of the performance~~
24 ~~under the agreement is to occur may be so utilized as to that~~
25 ~~part of the performance.~~

1 ~~(e) The express terms of an agreement [including terms~~
2 ~~to which a party has manifested assent] and any applicable course~~
3 ~~of performance, course of dealing, or usage of trade must be~~
4 ~~construed wherever reasonable as consistent with each other. If~~
5 ~~such a construction is unreasonable.~~

6 ~~(1) express terms prevail over course of~~
7 ~~performance, course of dealing, and usage of trade;~~

8 ~~(2) course of performance prevails over course of~~
9 ~~dealing and usage of trade; and~~

10 ~~(3) course of dealing prevails over usage of~~
11 ~~trade.~~

12 ~~(f) Evidence of a relevant usage of trade offered by~~
13 ~~one party is not admissible unless that party has given the other~~
14 ~~party such notice as the court finds sufficient to prevent unfair~~
15 ~~surprise to the other party.~~

16 **Source:** Article 1 Draft Section 1-304.

17 **Committee Vote:** To delete this section Committee 5 Yes - 1 No
18 Observers 16 Yes - 0 No

19 **Reporter's Note:** The Committee voted to delete this section
20 consistent with its policy determination that this Act should be
21 as strictly procedural in its effect as possible. The view of
22 the Committee was that the question of usage evidence as
23 informing the substance of an agreement was an issue best left to
24 the underlying substantive law of the transaction. Since the
25 overarching theme of this Act is simply to effectuate an
26 alternative means to consummate and perform transactions, the
27 construction of the agreements reached in those transactions is
28 to be left to the underlying law applicable to the particular
29 transaction.

30 The commentary will make clear that the absence of a
31 provision relating to the employment of usage evidence as a means
32 of construction is in no way intended to remove such
33 considerations when otherwise relevant under the substantive law
34 applicable to the transaction.

1 **[SECTION 1078. MANIFESTING ASSENT.** In a transaction governed by
2 this [Act], the following rules apply:

3 (a) A person or electronic agent manifests assent to a
4 record or term ~~in a record~~ if, acting with knowledge of the
5 ~~terms~~ or after having an opportunity to review the record or
6 term ~~under Section 109,~~ it:

7 (1) signs the record or term ; or

8 (2) engages in ~~other~~ affirmative conduct or operations
9 that the record clearly provides the or the circumstances , including
10 the terms of the record , clearly indicate the will constitute
11 acceptance , and the person or electronic agent had an opportunity
12 to decline to engage in the conduct or operations. ~~of the record~~
13 ~~or term; and~~

14 ~~(2) had an opportunity to decline to sign the record~~
15 ~~or term or engage in the conduct.~~

16 (b) ~~The m~~Mere retention of information or a record without
17 objection is not a manifestation of assent.

18 (c) If assent to a particular term ~~in addition to assent to~~
19 ~~a record~~ is required by the substantive rules of law governing
20 the transaction, a person's conduct or electronic agent does not
21 manifest assent to ~~that~~ the term unless there was an opportunity
22 to review the term and the ~~signature or conduct~~ manifestation of
23 assent relates specifically to the term.

24 (d) A manifestation of assent may be proved in any manner,
25 including ~~by~~ showing that a procedure existed by which a person
26 or an electronic agent must have engaged in conduct or operations

1 that manifested~~s~~ assent to the record or term in order to proceed
2 further in the transaction.]

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

4 **Notes to This Draft:** Edited to more closely track Article 2B and
5 to establish the concept of manifesting assent as a procedural
6 mechanism for demonstrating agreement to a record or term.

7 **Reporter's Note:** At the January meeting express reference to
8 manifestation of assent was removed from the substantive
9 provisions of this Act in Sections 302 and 401. The section has
10 been retained in brackets for further discussion in light of
11 comment at the January meeting that it may be appropriate to
12 retain the section as a procedural provision. The idea is to
13 retain the concept in a way which indicates "how," in an
14 electronic environment, parties may show manifestation of assent
15 to a record or term. In light of the Committee's desire to leave
16 the determination of what amounts to agreement to other,
17 substantive law, it seems appropriate to establish a method
18 outlining the manner in which parties can establish the
19 "manifestation of mutual assent" referenced in Restatement 2d
20 Contracts Section 3.

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

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

37 The situations where parties participate in detailed
38 negotiations leading to the formation of an integrated contract
39 setting forth all the terms to which both parties have agreed are
40 largely limited to transactions involving large amounts. Even
41 outside the electronic environment, the use of pre-printed
42 standard forms has supplanted detailed negotiations in many small
43 amount transactions. Accordingly the concept of manifesting
44 assent to a record or terms of a record has supplemented the
45 notion of actual agreement in determining that to which the
46 parties have agreed to be bound (See Restatement (Second)
47 Contracts Section 211, UCC Section 2-207).

48 Even in an electronic environment it remains possible to
49 negotiate to agreement. In such a case, if parties engage in e-
50 mail correspondence which results in a classic offer and

1 acceptance of the terms (and only the terms) set forth in the
2 correspondence, the electronic signatures appended to the e-mail
3 messages serve to authenticate the records and result in contract
4 formation. This is the case since an electronic signature, by
5 definition, is made with intent to authenticate the record.

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

22 A provision dealing with manifesting assent is particularly
23 useful in the electronic environment where the real possibility
24 of a contract being formed by two machines exists. Although
25 Sections 302 and 401 no longer expressly refer to manifestation
26 of assent, the concept remains applicable in determining when a
27 signature occurs and what the terms of an agreement are when
28 contracts or signatures result from the operations of electronic
29 agents, either between electronic agents or when interacting with
30 a human.

31
32 **[SECTION 1089. OPPORTUNITY TO REVIEW.** A person or electronic
33 agent has an opportunity to review ~~a record or term~~ only if it
34 the record or term is made available in a manner that:

35 (a) which would call~~s~~ it to the attention of ~~the~~ a
36 reasonable person and permit~~s~~ review; or

37 (b) in the case of an electronic agent, would ~~of its terms~~
38 ~~or enables~~ a reasonably configured ~~the~~ electronic agent to react
39 ~~to it.~~]

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

41 **Notes to This Draft:** Edited to more closely parallel Article 2B.

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

1 **SECTION 10910. DETERMINATION OF COMMERCIALY REASONABLE SECURITY**
2 **PROCEDURE; ~~COMMERCIALY UNREASONABLE SECURITY PROCEDURE; NO~~**
3 **~~SECURITY PROCEDURE.~~**

4 **[ALTERNATIVE 1]**

5 (a) The commercial reasonableness of a security procedure
6 is determined ~~by the court~~ as a matter of law in light of the
7 purposes of the procedure and the circumstances at the time the
8 parties agreed to or adopted the procedure including the nature
9 of the transaction, sophistication of the parties, volume of
10 similar transactions engaged in by either or both of the parties,
11 availability of alternatives offered to but rejected by a party,
12 cost of alternative procedures, and procedures in general use for
13 similar transactions.

14 (b) A security procedure established by law or regulation
15 ~~shall be determined to be~~ is commercially reasonable for the
16 purposes for which it was established.

17 **[ALTERNATIVE 2]**

18 (a) The commercial reasonableness of a security procedure is
19 determined as a matter of law.

20 (b) In making a determination about the commercial
21 reasonableness of a security procedure, the following rules
22 apply:

23 (1) A security procedure established by law or
24 regulation is commercially reasonable for the purposes for which
25 it was established.

1 (2) Except as otherwise provided in subsection (b) (1),
2 commercial reasonableness is determined in light of the purposes
3 of the procedure and the commercial circumstances at the time the
4 parties agree to or adopt the procedure.

5 (3) A commercially reasonable security procedure may
6 require the use of any security devices that are reasonable under
7 the circumstances.

8 ~~(b) If a loss occurs because a person complies with a~~
9 ~~security procedure that was not commercially reasonable, the~~
10 ~~person that required use of the commercially unreasonable~~
11 ~~security procedure bears the loss unless it disclosed the nature~~
12 ~~of the risk to the other person and offered commercially~~
13 ~~reasonable alternatives that the person rejected. The liability~~
14 ~~of the person that required use of the commercially unreasonable~~
15 ~~security procedure is limited to losses that could not have been~~
16 ~~prevented by the exercise of reasonable care by the other person.~~

17 ~~(c) Except as otherwise provided in subsection (b), Section~~
18 ~~202, Section 203, or Section 302, if a loss occurs because no~~
19 ~~security procedure was used, the person relying on an electronic~~
20 ~~record or electronic signature as between the two parties, the~~
21 ~~party who relied bears the loss.~~

22 **Source:** Alternative 1 - UETA 110(a and b) (Nov. 25, 1997 Draft)
23 and Illinois Model Section 303(a); Alternative 2 - Article 2B
24 Draft Section 2B-114.

25 **Reporter's Note:** This section separates the issue of the
26 commercial reasonableness of a security procedure from the issue
27 of the effect of imposition of a commercially unreasonable
28 security procedure in the next section. This permits exclusion

1 of the terms of this section from the general rule under this
2 draft that the terms of this Act may be varied by agreement
3 (Section 105).

4 Two alternatives are provided for the Committee's
5 consideration. Alternative 1 is an edit of prior section 110(a).
6 This alternative more fully sets forth the considerations which
7 will be taken into account in determining the commercial
8 reasonableness of a security procedure. Alternative 2 comes from
9 the March, 1998 draft of Article 2B. The substance of subsection
10 (b)(3) is included in the last sentence of the definition of a
11 security procedure in UETA Section 102(a)(19).

12 In response to comments expressing concern about assigning
13 this determination, possibly viewed as a fact question reserved
14 to the finder of fact, "to the court", both alternatives provide
15 that the determination of commercial reasonableness is made as "a
16 matter of law", rather than as a decision "by the court."

17 **SECTION 110. EFFECT OF REQUIRING A COMMERCIALLY UNREASONABLE**
18 **SECURITY PROCEDURE.**

19 **[ALTERNATIVE 1]**

20 _____ (a) If a person (the "requiring party") requires, as a
21 condition of entering into a transaction with another person,
22 that the parties use a security procedure which is not
23 commercially reasonable, the following rules apply:

24 _____ (1) If the other party reasonably relies to its
25 detriment on an electronic record or electronic signature
26 purporting to be that of the requiring party, the requiring party
27 is estopped to deny the source or informational integrity of the
28 electronic record or authenticity of the electronic signature to
29 which the security procedure was applied; and

30 _____ (2) If the requiring party receives an electronic
31 record or electronic signature purporting to be that of the other
32 party, the requiring party will not be entitled to the benefit of
33 any presumption which may arise under Sections 202, 203 or 302.

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

4 **[ALTERNATIVE 2]**

5 (a) Subject to subsection (b) and Section 202, as between
6 parties to a security procedure, a party that requires use of a
7 security procedure that is not commercially reasonable is
8 responsible for losses caused by reasonable reliance on the
9 procedure in a transaction for which the procedure was required.

10 (b) The responsibility of the party that requires use of the
11 commercially unreasonable security procedure is limited to losses
12 in the nature of reliance and restitution. The party's
13 responsibility does not allow a double recovery for the same loss
14 and does not extend to:

15 (1) loss of expected benefit, including consequential
16 damages;

17 (2) losses that could have been prevented by the
18 exercise of reasonable care by the other party; or

19 (3) a loss, the risk of which was assumed by the other
20 party.

21 (c) A person does not require a procedure under subsection
22 (a) if it makes commercially reasonable alternative procedures
23 available to the other person.

24 **Source:** Alternatives 1 and 2 are both new based on consultation
25 between the Article 2B Reporter and Committee Chair and the UETA
26 Reporter and Committee Chair. Alternative 1 was drafted by the
27 UETA Reporter in consideration of the discussions regarding
28 former section 110(b) at the January meeting. Alternative 2 is
29 from the March, 1998 Draft of Article 2B.

1 **Reporter's Note:**

2 General Policy: This section is intended to impose liability and
3 create strong disincentives for the imposition of the use of
4 security procedures which are not commercially reasonable. This
5 section, under either alternative, is intended to apply only in
6 the case where the requiring party is in a position to, and in
7 fact does impose the use of the commercially unreasonable
8 procedure. As noted in subsection (3), if the parties negotiate
9 or jointly select a procedure, or have commercially reasonable
10 alternatives available, this section would have no application.
11 In such a case, or indeed in cases where no security procedure is
12 used, resulting losses are allocated in accordance with the
13 applicable substantive law outside this Act.

14 At the January meeting concern was raised that the liability of a
15 party for imposition of a commercially unreasonable security
16 procedure was predicated on the imposer failing to disclose risks
17 and offer alternatives. Under subsection (c) of each
18 alternative, by offering commercially reasonable alternatives,
19 the imposer may avoid operation of this section.

20 **Alternative 1 - Structure.**

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

29 Where a person requires, as a condition of doing business,
30 a security procedure which cannot be shown to be commercially
31 reasonable, an imposition has occurred and losses resulting from
32 the other party's detrimental reliance will be borne by the
33 requiring person under this section. Alternative 1 places the
34 loss on the requiring party through the use of estoppel and
35 denial of the benefits of presumptions created by this Act. This
36 structure is intended to avoid the creation of substantive
37 allocation rules regarding the types of losses which may result.
38 While preventing an imposing party from any benefits resulting
39 from reliance on a commercially unreasonable procedure, this
40 section leaves to the underlying substantive law applicable to
41 the particular transaction, the actual determination of the type,
42 amount and extent of recoverable losses. The following
43 illustrations suggest the manner of the operation of Alternative
44 1.

45 The easy cases - The requiring party is the recipient of the
46 record:

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

8 **Illustration 2.** Same facts as Illustration 1. Through no
9 fault of franchisee, bad guy sends an electronic record,
10 showing franchisee's E-mail as the identifier, ordering
11 \$100,000 of merchandise from GM to be shipped to the bad
12 guy. The procedure would not be commercially reasonable.
13 If the underlying agreement as to the procedure were
14 controlling, the franchisee would bear the loss, since the
15 electronic record would be attributable to the franchisee.
16 Since this is an imposed, commercially unreasonable
17 procedure, the \$100,000 loss arising directly from the
18 transaction would be suffered by GM because GM would be
19 unable to establish that the order was attributable to the
20 franchisee under Section 202.

21 **Illustration 3.** Same facts as Illustration 2. If the bad
22 guy is an employee of the franchisee the result, in this
23 case, should be no different. The procedure is so open that
24 the franchisee would have to somehow "lock up" all its
25 computers to deny the employee the ability to send an order
26 on behalf of the franchisee. Unless GM could establish
27 attribution in fact under Section 202(a)(1) [or lack of
28 reasonable care by franchisee under Section 202(b)], GM
29 would bear the loss.

30 **Illustration 4.** Franchisee places a \$100,000 order with GM.
31 A bad guy hacks into GM's computer and learns of the order
32 and the timing and method of shipment. The bad guy
33 intercepts the shipment and steals it. While GM may be
34 liable for negligence in the custody of its order records,
35 this section is not applicable. Although there was a
36 commercially unreasonable procedure, the loss in this case
37 was not caused by the laxity of the procedure. If GM is
38 able to prove that the order came from the franchisee
39 (unaided by the presumption in 202 because the procedure is
40 not commercially reasonable), the loss would be determined
41 under Article 2 or general contract principles.

42 The more difficult cases - The requiring party is the sender of
43 the record:

44 **Illustration 5.** GM requires all of its suppliers to do
45 business using only GM's e-mail address as the identifier.
46 Bad guy sends an e-mail showing GM's address as the
47 identifier ordering \$50,000 of parts. Supplier reasonably

1 relies on the e-mail and ships the goods. Bad guy
2 intervenes and takes the goods. In Supplier's claim for
3 payment, GM will be estopped to deny that it sent the order.
4 Without the ability to deny that the order was from GM,
5 supplier may hold GM liable as though the contract had been
6 formed, upon proof of supplier's performance, etc, under the
7 substantive law of sales.

8 **Illustration 6.** Same procedure as in Illustration 5. GM
9 actually sends order and supplier ships. As in Illustration
10 4, Bad guy learns of the shipment and intervenes and steals
11 the shipment. Here the only question is risk of loss under
12 applicable sales and contract law.

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

22 In a consumer context the general result will be that a vendor
23 receiving an order will bear the risk that the order did not come
24 from the purported sender. If a commercially reasonable security
25 procedure is used by the vendor, the consumer would likely adopt
26 the procedure in order to complete the transaction and the vendor
27 would receive the benefit of the presumptions under this act.
28 The following are somewhat atypical illustrations:

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

40 **Illustration 9.** Buyer logs on to an internet vendor. In
41 placing the order it uses a commercially unreasonable
42 security procedure. Vendor has not agreed to the procedure
43 but does adopt it by processing the order. This section
44 does not apply. No presumptions attach since the procedure
45 was commercially unreasonable, and the parties are left to
46 deny or prove up the resulting contract.

1 As indicated by the illustrations, the question of the extent of
2 damage recovery by any party is left entirely to other law. The
3 effect of a commercially unreasonable procedure that is imposed
4 by one party is simply to raise estoppel or deny presumptions.
5 After application of an estoppel, the transaction is proven or
6 denied by other means and the resulting liability determined
7 pursuant to other substantive law.

8 Alternative 2 adopts a different approach to the problems
9 raised by requiring commercially unreasonable procedures. It
10 addresses the liability of the requiring party and limits the
11 extent of the losses covered. The following is the Article 2B
12 Reporter's Notes explaining the operation of Alternative 2.

13 **ARTICLE B REPORTER'S NOTES:**

14 **Notes to this Draft:**

15 This Section was revised based on consultation with the
16 Electronic Transactions Reporter and Committee chair and in
17 light of the discussion of the issues during the February
18 1998 meeting.

19 **General Notes:**

20 1. General Policy and Scope. This section deals with
21 allocation of loss in cases where one party (either the
22 licensor or the licensee) requires use of an attribution
23 procedure that is commercially unreasonable and use of that
24 procedure causes a loss either because of undetected errors
25 in transmissions or records or because of third party
26 activity in the nature of fraud or otherwise. The Section
27 does not cover all cases in which such loss might occur, but
28 deals only with circumstances in which a party is in a
29 position to and does in fact require use of the commercially
30 unreasonable procedure. A procedure negotiated or jointly
31 selected by the parties, selected from among alternatives
32 that include a commercially reasonable option, or mutually
33 designed, does not fall within this Section. Responsibility
34 for loss in such cases lies outside this article.

35 a. Reliance Loss. The basic premise is that, all
36 things being otherwise equal, loss in the nature of reliance
37 or restitution should fall on the party that required use of
38 the procedure that caused the loss. This is a contract
39 statute, not a general regulatory or tort liability statute
40 and, thus, the losses to which it applies are limited to
41 situations in which loss results from use of the procedure
42 in a transaction to which the requirement applies.

43 b. Transactions Not Affected. Additionally,
44 since this entire article deals with licensing and related
45 transactions, the losses are confined to such transactions.
46 The Section does not apply to credit card, funds transfer or
47 other types of transactions in which attribution procedures
48 are used, but which fall outside the scope of Article B and,
49 in many cases, are at least partially regulated by federal
50 or other state laws. Thus, for example, use of an

1 identifying code for a credit card payment is not governed
2 by this section. However, if a contracting party requires
3 that the other party use a credit card number as an
4 attribution procedure, credit card law applies as to the
5 payment transaction, but as to the contractual relationship,
6 Section B-115 applies if the procedure is regarded as
7 commercially reasonable and this Section applies if the
8 procedure was "required" and is commercially unreasonable.

9 c. Relationship to Reasonable Procedures. The
10 loss allocation principle expressed in this Section
11 contrasts to the principles stated in Section B-116 and B-
12 117. Those sections provide the parties with presumptions
13 about the authenticity and accuracy of the electronic
14 records to which the procedures are applied. The
15 presumptions are potentially significant in litigation and
16 planning transactions. As expressed there, the presumptions
17 arise only if the procedure is commercially reasonable.
18 Thus, a commercially reasonable procedure vitiates the
19 presumption, leaving the parties to general proof of content
20 and source of the record. In addition, if the procedure
21 comes within this section, the use of an unreasonable
22 procedure may have an impact on loss allocation.

23 2. Party Responsible. The section refers to the person that
24 required the procedure as being responsible for the loss.
25 In modern commerce, the person making such requirement is in
26 some cases the licensor and in some cases the licensee. The
27 principle used here applies in either direction. The
28 procedure must, however, be one that the parties have agreed
29 to or adopted. That elements is implicit in the definition
30 of what constitutes an "attribution procedure."

31 The Section does not necessarily create an
32 affirmative right of recovery. In some cases, the Section
33 merely denies the relying party an ability to recover from
34 the other person. Thus, for example, a licensor acting
35 pursuant to a commercially unreasonable attribution
36 procedure, might ship information product to a third party
37 that used the inadequacies of the procedure to dupe the
38 licensor into believing that the party requesting shipment
39 was the named licensee. If the licensor had required the
40 procedure and the licensee had agreed to it for transactions
41 of this type, this Section allows the licensee to resist any
42 effort by the licensor to charge the licensee for the loss
43 or the contract price. The licensor remains responsible.
44 On the other hand, if the licensee had required the
45 procedure and the licensor agreed to it, the licensor may
46 recover against the licensee for the losses in the nature of
47 reliance. It cannot, of course, in this case seek recovery
48 under contract theory since the licensee did not make the
49 purchase request..

50 3. Type of Loss, The loss to which this Section
51 applies is limited in several ways.

1 The loss must, initially, come from use of the
2 procedure. This excludes losses that flow from other,
3 perhaps parallel causes. Thus, if an identifier is
4 unreasonable, but the party actually did engage in the
5 transaction, but suffered loss due to a breach of contract,
6 this section does not apply. The losses addressed here are
7 in the nature of loss from misattribution of who sent a
8 message, tampering with the content of a message, or errors
9 caused by transmission or other factors.

10 Second, the Section only applies to losses
11 incurred in transactions to which the requirement and use of
12 the procedure between the parties applies. It does not
13 address the difficult problem of liability for the situation
14 where a third party wrongdoer obtains social security or
15 other important identifies of an innocent third party and
16 uses them to fraudulently obtain goods and services from
17 numerous vendors. That issue lies in the realm of tort law,
18 criminal law, and other forms of regulation that are just
19 now beginning to develop. Of course, to the extent that
20 these other sources of law preempt or preclude operation of
21 this section, ordinary preemption rules apply.

22 Third, the losses do not include lost benefits of
23 the transactional relationship. They are limited to
24 reliance and restitution recovery. In some cases, however,
25 the existence and non-performance of a contractual
26 relationship may allow expectations recovery. The basic
27 premise here, however, is limited to avoiding a shift of
28 losses through a required procedure that fails to protect
29 the interests of the parties.

30 The emphasis on reliance recovery, of course,
31 places further limitations on the recovery. These are
32 stated in subsection (b)(2) based on a lack of reasonable
33 care and an assumption of risk.

34 4. Illustrations. The following suggest some applications
35 of this Section.

36 a. False Identity Cases: No Contract. In many cases
37 where a loss is suffered by a party because a third party
38 fraudulently used an attribution identifier and order
39 information claiming to be the appropriate party, this Section
40 produces results that are parallel to the results that could
41 be inferred under other attribution rules of this Article.

42 **Illustration 1.** S (the vendor) required and M agreed to a
43 procedure for identifying M in placing orders with S. Thief
44 misuses this procedure and, purporting to be M, obtains a
45 \$10,000 electronic encyclopedia from S. S, believing that M
46 placed the order, seeks the license fee from M. Under the
47 general attribution sections, if the procedure is not
48 commercially reasonable, there is no presumption that the
49 sender was M and, since M can prove it was not the sender,
50 it has no liability. Under this section, the required
51 attribution procedure caused a loss, but S is responsible
52 for that loss. It cannot shift loss to M.

1 In some false identity cases, however, the party
2 demanding the use of the attribution procedure may be
3 responsible for affirmative losses.

4 **Illustration 2.** M (the purchaser) requires L to use a
5 procedure under which M identifies itself when placing
6 orders with L. Thief uses the procedure to fraudulently
7 obtain a \$10,000 software system from L. Under this
8 Section, since M required use of the procedure and it was
9 commercially unreasonable, the loss suffered may be
10 recovered from M. The amount of loss is measured by
11 reliance, not lost profit. In essence, the recovery is the
12 cost (not license price) of the software shipped to the
13 thief plus related expenses.

14 b. True Contract: Errors in Performance. In
15 cases where an actual contract exists between the parties
16 and the error or fraud allowed by the unreasonable
17 attribution procedure relates to performance, it will often
18 be the case that contract remedies provide the primary
19 recovery and, under the principle that precludes double
20 recovery, the reliance loss allocation of this does not
21 create affirmative recovery. It nevertheless confirms the
22 placement of ultimate losses in such cases.

23 **Illustration 3.** L (licensor) and M (licensee) agree to a
24 license for a \$10,000 commercial software license. L
25 requires M to agree to a procedure for sending instructions
26 as to where to transmit the software. M pays the license
27 fee. A third party intervenes and causes misdirection of the
28 software copy. M demands its software. Under this Section,
29 L would bear responsibility for reliance or restitution
30 loss. M can recover the fee it paid. More generally,
31 however, M can enforce the unperformed contract and, in the
32 event of breach, can recover contract damages, including
33 consequential damages, as appropriate.

34 **Illustration 4.** In the Illustration 3, assume that M did
35 in fact direct the transmission of the software, but now
36 denies that it did so. If the procedure had been
37 reasonable, L would have the advantage of a presumption of
38 attribution of the message. Since it was not, L must prove
39 that M did send the message without the benefit of a
40 presumption. If it can do so, it can enforce the contract.
41 Under this section, M suffered no loss due to the
42 attribution procedure.

43 c. Errors in the Offer and Acceptance. The
44 problem of garbled, misrecorded or otherwise mistaken offers
45 and acceptances is one of long-standing in commercial
46 practice. This Section provides a method of allocating loss
47 in such cases based on the reasonableness of the required
48 procedure and independent of asking arcane questions about
49 what terms were accepted and when,.

50 **Illustration 4[5].** M requires that L use an unreasonable
51 attribution procedure for transmitting orders and
52 acceptances. L agrees and adopts the procedure. It places

an order for ten software widgets. Because the procedure is flawed, the message arrives at M requesting 100 software widgets. M ships on that basis. L desires to ship the ninety excess widgets back to M and not pay. One could argue that no contract exists because of mistake. Alternatively, a contract might be formed on the offer as sent or as received. Case law support exists for either result. This section, however, focuses on reliance loss. Either L or M could be said to suffer loss because of reliance on the procedure. Since M required it, M bears responsibility for the loss. It cannot demand the price for the ninety widgets unless, of course, L decides to accept and retain them. If L had required the use of the procedure, it would be responsible for reliance losses and restitution.

END OF ARTICLE B REPORTER NOTES

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.

~~SECTION 111. OBLIGATION OF GOOD FAITH. There is an obligation to act in good faith in the formation, performance, and enforcement of every transaction and duty within the scope of this [Act].~~

Source: Revised Article 1 Section 1-305 (Sept. 1997 Draft)

Committee Vote: To delete this section Committee Yes 6 - No 1
Observers Yes 7 - No 5

Reporter's Note: This section, added in response to comments at the September Meeting, was deleted by the Committee at the January meeting. The section was viewed as creating substantive requirements best left to the substantive law of the transaction.

~~SECTION 112. GENERAL PRINCIPLES OF LAW APPLICABLE.~~

~~Unless displaced by the particular provisions of this [Act], the principles of law and equity, including the law merchant and the law relating to contract, principal and agent, estoppel, fraud, misrepresentation, duress, coercion, mistake, bankruptcy and other validating and invalidating cause shall supplement its provisions.~~

1 **Source:** UCC Section 1-103

2 **Committee Vote:** To delete this section and incorporate its
3 substance as a subsection to Section 103 Scope. Unanimous
4 approval by both the Committee and Observers.

5 **Reporter's Note:** This section was added based on comments at the
6 September Meeting. The substance of this section has been
7 incorporated as Subsection 103(b). The language used in 103(b)
8 is the new language from Revised Article 1. The Committee moved
9 this provision to make clear that the scope of this Act is
10 limited and that the general principles of substantive law are
11 to be applied to transactions governed by this act.

12 **PART 2**

13 **ELECTRONIC RECORDS GENERALLY**

14 **SECTION 201. LEGAL RECOGNITION OF ELECTRONIC RECORDS.**

15 (a) A record may not be denied legal effect, validity, or
16 enforceability solely because it is ~~in the form of~~ an electronic
17 record.

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

21 (c) In any transaction, a ~~A~~ person may establish reasonable
22 requirements regarding the type of records ~~which will be~~
23 acceptable to it.

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

26 **Reporter's Note:**

27 1. Part 2 reflects the fundamental reorganization of this Act
28 in the November, 1997 Draft. Part 2 now deals with those
29 provisions relating to the validity, effect, and use of
30 electronic records, Part 3 contains those sections dealing with
31 the validity and effect of electronic signatures, and Part 4
32 reflects general contract provisions, and provisions dealing with
33 the effect of both electronic records and electronic signatures.
34 Under different provisions of substantive law the legal effect
35 and enforceability of an electronic record may be separate from
36 the issue of whether the record contains a signature. For
37 example, where notice must be given as part of a contractual

1 obligation, the effectiveness of the notice will turn on whether
2 the party provided the notice regardless of whether the notice
3 was signed. An electronic record attributed to a party under
4 Section 202 would suffice in that case, notwithstanding that it
5 may not contain a signature.

6 2. This section reflects a merger of former Sections 201 and
7 202 from the August Draft.

8 3. Subsection (a) establishes the fundamental premise of this
9 Act: That the form in which a record is generated, presented,
10 communicated or stored may not be the only reason to deny the
11 record legal recognition. On the other hand, subsection (a)
12 should not be interpreted as establishing the legal
13 effectiveness, validity or enforceability of any given record.
14 Where a rule of law requires that the record contain minimum
15 substantive content, the legal effect, validity or enforceability
16 will depend on whether the record meets the substantive
17 requirements. However, the fact that the information is set
18 forth in an electronic, as opposed to paper record, is
19 irrelevant.

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

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

36 **Illustration 2:** A sends the following e-mail to B: "I
37 hereby offer to buy 100 widgets for \$1000, delivery next
38 Tuesday. /s/ A." B responds with the following e-mail: "I
39 accept your offer to purchase 100 widgets for \$1000,
40 delivery next Tuesday. /s/ B." In this case the analysis is
41 the same as in Illustration 1 except that here the records
42 otherwise satisfy the requirements of CC Section 2-201(1).
43 The transaction may not be denied legal effect solely
44 because there is not a pen and ink "writing."
45

46 The purpose of the Section is to validate electronic records in
47 the face of legal requirements for paper writings. Where no

1 legal requirement of a writing is implicated, electronic records
2 are subject to the same proof issues as any other evidence.

3 5. Subsection (c) is a particularized application of Section
4 105, to make clear that parties retain control in determining the
5 types of records to be used and accepted in any given
6 transaction. For example, in the Chrysler recall hypothetical
7 referred to in Note 2 to Section 105, although Chrysler cannot
8 unilaterally require recall notices to be effective under this
9 Act, it may indicate the method of recall in a purchase agreement
10 with a customer. If the customer objects, the customer would
11 have the right to establish reasonable requirements for such
12 notices.

13 **SECTION 202. ATTRIBUTION OF ELECTRONIC RECORD TO A PARTY.**

14 (a) ~~As between the parties, a~~An electronic record is
15 attributable to a party person if:

16 (1) it was in fact the action of that party person,
17 ~~its agent~~a person authorized by it, or ~~its~~the person's electronic
18 agent;

19 (2) the other party person, in good faith and acting
20 in compliance with a commercially reasonable security procedure
21 for identifying ~~the party~~ the person to which the electronic
22 record is sought to be attributed, reasonably concluded that it
23 was the action of the other party person, ~~its agent~~a person
24 authorized by it, or ~~its~~the person's electronic agent, ~~or~~

25 (b) Attribution of an electronic record to a party person
26 under subsection (a) (2) has the effect provided for by the
27 agreement regarding the security procedure and, in the absence of
28 terms about such effect, creates a presumption that the
29 electronic record was that of the party person to which it is
30 attributed.

1 ~~[(c3)~~ Even if an electronic record is not attributable to a
2 person under subsection (a), a person ("responsible person") is
3 liable for losses in the nature of reliance, if the losses occur
4 because the electronic record:

5 (1) the responsible person failed to exercise
6 reasonable care;

7 (2) the other person ("relying person") reasonably
8 relied on the belief that the responsible person was the source
9 of the electronic record;

10 (3) that reliance~~(A)~~ resulted from acts of a third
11 person that obtained access to a security procedure, access
12 numbers, codes, computer programs, or the like, from a source
13 under the control of the party responsible person; and

14 (4) the use of the access numbers, codes, computer
15 programs or the like created~~ing~~ the appearance that the
16 electronic record came from the party responsible person.]7

17 ~~(B) the access occurred under circumstances~~
18 ~~constituting a failure to exercise reasonable care by the party~~
19 ~~person; and~~

20 ~~(C) the other party~~ person ~~reasonably relied to~~
21 ~~its detriment on the apparent source of the electronic record.~~

22 ~~(b) In a case governed by subsection (a) (3), the following~~
23 ~~rules apply:~~

24 ~~(1) The relying party has the burden of proving~~
25 ~~reasonable reliance, and the party to which the electronic record~~
26 ~~is to be attributed has the burden of proving reasonable care.~~

1 ~~(2) Reliance on an electronic record that does not~~
2 ~~comply with a security procedure is not reasonable unless~~
3 ~~authorized by an individual representing the party to which the~~
4 ~~electronic record is to be attributed.~~

5 **Source:** Article B Draft Section B-116.

6 **Notes to this Draft:** Edited for clarity and to more closely
7 track Article 2B Section 2B-115.

8 **Reporter's Note:** This section follows Article 2B and sets forth
9 risk allocation rules in the context of record attribution. The
10 section sets forth rules establishing the circumstances under
11 which a party will be bound by (be attributable for) an
12 electronic record sent to another party.

13 Subsection (a)(1) relies on general agency law, including
14 the new concept of electronic agency, to bind the sender.
15 Subsection (a)(2) deals with allocations of risk where security
16 procedures are involved and properly implemented. Under
17 subsection (a)(2) an electronic record will be attributed to the
18 sender if the recipient complied, in good faith, with a
19 commercially reasonable security procedure which confirmed the
20 source of the electronic record.

21 Subsection (b) provides a rebuttable presumption of
22 attribution where a security procedure is properly used. This
23 presumption is appropriate because of the definition of security
24 procedure which is now limited to procedures adopted by the
25 parties or established by law, and under this section, which are
26 also commercially reasonable. As Section 110 makes clear, where
27 a security procedure is shown to be commercially unreasonable,
28 the presumption will not apply and the loss generally will fall
29 on the relying party. Subsection (b) also makes clear that the
30 parties may alter the effect of the presumption, and provides a
31 default rule where the parties do not provide otherwise.

32 **Subsection (c)** is part of the March Draft of Article 2B but
33 **has been bracketed here for the Committee's consideration.** In
34 substance it appeared as subsection (a)(3) in the prior drafts of
35 both this act and Article 2B, with the result that in the case of
36 negligence an electronic record could be attributed to, and
37 therefore binding upon, a party. The substance of this
38 subsection does not truly address the issue of attribution and
39 has been properly set off as a separate basis for liability. It
40 is more in the nature of a direct loss allocation provision
41 rather than an attribution provision. Under subsection (c) when
42 the negligence of one party, together with reasonable reliance by
43 the other party caused by the negligence, results in loss to the
44 relying party, the negligent party bears losses "in the nature of
45 reliance." Like Alternative 2 to Section 110 regarding the
46 effect of requiring a commercially unreasonable security
47 procedure, this section implicates substantive loss allocation

determinations. Considering the Committee's apparent desire to avoid such substantive effects, it may be possible to redraft this subsection along the lines of Alternative 1 to Section 110.

SECTION 203. DETECTION OF CHANGES AND ERRORS. ~~(a) If through a~~
the parties act in compliance with a commercially reasonable
security procedure to detect errors or changes in the
informational content of an electronic record, between the
parties the following rules apply:

~~(a) the informational content of a~~An electronic record that
the security procedure shows ~~can be shown~~ to have been unaltered
since a specified point in time, ~~the informational content shall~~
~~be~~ is presumed to have been unaltered since that time.

(b) ~~If a~~An electronic record is created or sent in
accordance with ~~a~~ the security procedure ~~for the detection of~~
~~error, the informational content in the electronic record is~~
presumed to have the informational content ~~be as~~ intended by the
person creating or sending it as to portions of the informational
content to which the security procedure applies.

~~(c) If the electronic record nevertheless contained an~~
~~error but the error was not discovered, the following rules~~
~~apply:~~

~~(1)~~ If the sender complied with the security
procedure, but the other party did not, and the change or error
would have been detected had the ~~receiving~~ other party also
complied with the security procedure, the sender is not bound by
the error or change.

1 ~~(d)(2)~~ If the ~~sender receives a notice~~ other party notifies
2 the sender in a manner required by the security procedure that
3 describes the informational content of the record as received,
4 the sender shall review the notification~~ce~~ and report any error
5 detected by it in a commercially reasonable manner. Failure to
6 so review and report any error ~~shall~~ binds the sender to the
7 informational content of the record as received.

8 **Source:** Article 2B Draft Section 2B-117

9 **Notes to this Draft:** Edited for clarity and to more closely
10 track Article B.

11 **Reporter's Note:**

12 1. Like Section 202, this section allocates the risk of errors
13 and changes in transmission to the party that could have best
14 detected the error or change through the proper application and
15 use of a security procedure. Again, since the parties will have
16 agreed or adopted the security procedure, the creation of the
17 presumption of accuracy, and allocation of risk to the party that
18 should have discovered the error, should not pose undue hardship
19 or unfair surprise on the party bearing the loss.

20 **[SECTION 204. INADVERTENT ERROR. (a) In this section,**
21 "inadvertent error" means an error by an individual made in
22 dealing with an electronic agent of the other party when the
23 electronic agent of the other party did not allow for the
24 correction of the error.

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

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

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

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

10 ~~(cd) In subsection (bc), the burden of proving intent and~~
11 ~~lack of error is on the other party, and the individual has the~~
12 ~~burden of proving compliance with subsections (bc) (1), (2), and~~
13 ~~(3).]~~

14 **Source:** UETA Section 203(c-e) (Nov. 1997 Draft)

15 **Notes to this Draft:** This provision has been moved to a new
16 section for clarity.

17 **Reporter's Notes:** Section 2B-117(c) of the November 1, 1997 draft
18 of Article 2B created a new, rather elaborate defense for
19 consumers when errors occur. This section now appears as Section
20 2B-118 of the March Draft. As currently drafted the defense
21 relates to errors occurring because of system failures. Whether
22 2B-118 addresses human error (as in the single stroke error of
23 concern to a number of observers at the September Meeting) could
24 be clearer, although the recent draft and Illustration 2 to that
25 section, suggest that what is termed "inadvertent error" here is
26 covered. Because the allocation of losses under this draft turns
27 on the use of security procedures and their commercial
28 reasonableness and places the loss on the party choosing to rely
29 on electronic records and electronic signatures, the distinction
30 between consumers and merchants, and sophisticated and
31 unsophisticated parties has been eliminated. Rather the burden
32 is placed on the person consciously desiring the benefits of
33 electronic media to assure that the level of security necessary
34 exists.

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

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

10 Subsection (c) has been deleted in this draft. The issue of
11 the burden of proof should be left to the law of pleading and
12 evidence. In any event, the provisions in subsection (c) did not
13 alter what would otherwise be the burdens in litigation.

14 **THE QUESTION FOR THE DRAFTING COMMITTEE is whether this section**
15 **is appropriate and should be retained? A second question is**
16 **whether the section should be expanded to cover systems errors as**
17 **is the case under 2B-118?**

18
19 **SECTION 2054. ORIGINALS: ACCURACY OF INFORMATION ACCURACY.**

20 (a) If a rule of law [or a commercial practice] requires a
21 record to be presented or retained in its original form, or
22 provides consequences ~~for~~ if the record is not ~~being~~ presented or
23 retained in its original form, that requirement is met by an
24 electronic record if [the electronic record is shown to reflect
25 accurately] [there exists a reliable assurance as to the
26 integrity of] the information set forth in the electronic record
27 from the time ~~when~~ it was first generated in its final form, as
28 an electronic record or otherwise.

29 (b) The integrity and accuracy of the information in an
30 electronic record are determined by whether the information has
31 remained complete and unaltered, apart from the addition of any
32 endorsement and any change that arises in the normal course of
33 communication, storage, and display. The standard of reliability
34 required must be assessed in the light of the purpose for which

1 the information was generated and in the light of all the
2 relevant circumstances.

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

5 **Reporter's Note:** This section deals with the serviceability of
6 electronic records as originals. As was noted at the May
7 meeting, the concept of an original electronic document is
8 problematic. For example, as I draft this Act the question may
9 be asked what is the "original" draft. My answer would be that
10 the "original" is either on a disc or my hard drive to which the
11 document has been initially saved. Since I periodically save the
12 draft as I am working, the fact is that at times I save first to
13 disc then to hard drive, and at others vice versa. In such a
14 case the "original" may change from the information on my disc to
15 the information on my hard drive. Indeed, as I understand
16 computer operations, it may be argued that the "original" exists
17 solely in RAM and, in a sense, the original is destroyed when a
18 "copy" is saved to a disc or to the hard drive. In any event, the
19 concern focuses on the integrity of the information, and not with
20 its "originality." Given the recognition of this problem, the
21 title of the section has been expanded to reflect the concern
22 regarding the informational integrity of an electronic record;
23 integrity which is assumed to exist in the case of an original
24 writing.

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

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

1 they have been altered, which would be difficult to detect
2 in copies.

3 Since requirements for "originals" are often the result of
4 commercial practice and not an actual rule of law, the section
5 includes the bracketed language regarding requirements derived
6 from commercial practice. As a policy matter it is not at all
7 clear that legislation should override established commercial
8 practice. **THIS IS A QUESTION WHICH MUST BE RESOLVED BY THE**
9 **DRAFTING COMMITTEE.**

10 So long as there exists reliable assurance that the
11 electronic record accurately reproduces the information, this
12 section continues the theme of establishing the functional
13 equivalence of electronic and paper-based records. This is
14 consistent with Fed.R.Evid. 1001(3) and Unif.R.Evid. 1001(3)
15 (1974) which provide:

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

19 **THE BRACKETED ALTERNATIVES FOR TESTING THE RELIABILITY OF THE**
20 **INFORMATIONAL CONTENT OF AN ELECTRONIC RECORD ARE PROVIDED FOR**
21 **THE DRAFTING COMMITTEE'S CONSIDERATION.** At the May meeting
22 concern was expressed that the "reasonable assurance" standard
23 was too vague. The first alternative tracks the language in the
24 rules of evidence and focuses on the accuracy of the information
25 presented. The second alternative is the language appearing in
26 Section 204 of the Illinois Model.

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

32 **SECTION 2065. RETENTION OF ELECTRONIC RECORDS.**

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

36 (1) the information contained in the electronic record
37 remains accessible so as to be usable for subsequent reference;

38 (2) the electronic record is retained in the format in
39 which it was generated, stored, sent, or received, or in a format

1 that can be demonstrated to reflect accurately the information as
2 originally generated, stored, sent, or received; and

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

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

11 (c) A person may satisfy the requirement referred to in
12 subsection (a) by using the services of any other person, if the
13 conditions set forth in subsection (a) are met.

14 (d) ~~Nothing in t~~This section does not precludes any federal
15 or state agency from specifying additional requirements for the
16 retention of records, either written or electronic, subject to
17 the agency's jurisdiction.

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

19 **Reporter's Note:** At the May meeting concern was expressed that
20 retained records may become unavailable because the storage
21 technology becomes obsolete and incapable of reproducing the
22 information on the electronic record. Subsection (a)(1)
23 addresses this concern by requiring that the information in the
24 electronic record "remain" accessible, and subsection (a)(2)
25 addresses the need to assure the integrity of the information
26 when the format is updated or changed.

27 This section would permit parties to convert original
28 written records to electronic records for retention so long as
29 the requirements of subsection (a) are satisfied. Accordingly, in
30 the absence of specific requirements to retain written records,
31 written records may be destroyed once saved as electronic records
32 satisfying the requirements of this section.
33
34

- 1
- 2

2

3

4
5
6

7
8
9
0

- 1
- 2
- 3

45

6

7
8
9
0
1
2
3
4
5
6
7
8

9
0
1
2
3
4

1 3. This section, consistent with the existing UCC definition of
2 a signature as "any symbol executed or adopted by a party with
3 present intention to authenticate a writing," merely reiterates
4 for clarity the rule that an electronic record containing an
5 electronic signature satisfies legal requirements. The critical
6 issue in either the signature or electronic signature context is
7 what the signer intended by the execution, attachment or
8 incorporation of the signature into the record.

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

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

24 **SECTION 302. ELECTRONIC SIGNATURES: EFFECT AND PROOF.**

25 (a) Unless the circumstances otherwise indicate that a
26 party intends less than all of the effect, an electronic
27 signature ~~is intended to~~ establishes

28 (1) the signing party's identity~~;~~

29 (2) its adoption and acceptance of a record or a
30 term~~;~~ and

31 (3) the integrity of the informational content
32 ~~integrity~~ of the record or term to which the electronic signature
33 is attached or with which it is logically associated.

34 (b) If ~~the signing party executed or adopted the~~ an
35 electronic signature is executed or adopted in accordance with a

commercially reasonable security procedure for validating electronic signatures, the following rules apply:

(1) the electronic signature is presumed to be authentic and authorized; and

(2) the electronic record to which the electronic signature is attached or with which it is logically associated is presumed to be signed by the person to whom the electronic signature correlates signing party.

(c) Otherwise, aAn electronic signature not governed by subsection(b) may be proven in any manner, including by showing that-

(1) a procedure existed by which a partythe person or its electronic agent must of necessity have engaged in conduct or operations that signed, or manifested assent to, a the record or term in order to proceed further in the processing of the transaction., or

(2) the partyperson is bound by virtue of the operations of its electronic agent.

(c) The authenticity of, and authority to make, an electronic signature is admitted unless specifically denied in the pleadings. If the validity of an electronic signature is denied in the pleadings, the burden of establishing validity is on the person claiming validity.

Source: Article 2B Draft Section 2B-118(a and c); Illinois Model Section 203.

Committee Vote: To delete subsection (c) but retain its effect as a presumption. Committee Unanimous in favor - Observers 14 Yes - 2 No

Reporter's Note:

1 1. An electronic signature is any symbol or methodology adopted
2 with intent to sign a writing. This Act includes in the
3 definition of signature the attributes normally associated with a
4 pen and ink signature in order to make clear what a signer
5 intends by signing a document, i.e., to identify oneself, adopt
6 the terms of the signed record, and verify the integrity of the
7 informational content of the record which is signed. By
8 identifying the multi-purpose effect of a signature, this Act
9 clarifies the assumption as to the intent of one signing any
10 record. Subsection (a) simply applies this assumption to the
11 electronic signature. As with a signature on paper, the signing
12 party remains free to prove that the signing was intended to
13 accomplish only 1 or 2 of the normal purposes associated with a
14 signing.

15 2. Subsection (b) has been changed to delete the idea that an
16 electronic record is signed as a matter of law when a security
17 procedure is used. Instead it creates a presumption that an
18 electronic signature executed or adopted pursuant to a security
19 procedure is the authentic, authorized signature of the signing
20 party. The purpose of the change is to make clearer the effect
21 of an electronic signature and to make the operation of security
22 procedures in the signature context parallel to the operation of
23 security procedures in the record context, i.e., the creation of
24 a presumption. The presumption now also addresses authenticity
25 and authority, which were formerly addressed in subsection (c).
26

27 3. Subsection (c) provides that an electronic signature, not
28 governed by a security procedure under subsection (b) may be
29 proven in any manner including procedures necessitating the
30 adoption of a term or record, or that the party is bound by the
31 operations of its electronic agent (Section 303). By allowing
32 proof of an electronic signature by showing that a process
33 existed which had to be followed to obtain the results achieved,
34 the section addresses the increasingly common "point and click"
35 processes in on-line and on-screen programs.
36

37 4. Former subsection (c) has been deleted consistent with the
38 Committee's instructions. The substantive effect has been moved
39 to subsection (b) by creating a presumption of authority and
40 authenticity where a commercially reasonable security has been
41 used. Unless the validity of an electronic signature is denied
42 by the purported singer, the presumption will stand to establish
43 the authority and authenticity of the electronic signature.
44 However, if the purported signer denies the validity of the
45 signature, the presumption would be overcome, and the party
46 asserting validity must carry the burden of so establishing.

1 **SECTION 303. ~~[SIGNATURES BY]~~ [OPERATIONS OF] ELECTRONIC AGENTS.**

2 (a) A party that designs, programs, or selects an
3 electronic agent is bound by operations of its electronic agent.

4 (b) An electronic record resulting from the operations of
5 an electronic agent ~~shall be~~ is deemed to have been signed by the
6 party designing, programming, or selecting the electronic agent,
7 ~~regardless of whether~~ or not the operations result in the
8 attachment or application of an electronic signature to the
9 electronic record.

10 **Source:** Prior UETA Section 204(b) (August Draft)

11 **Reporter's Note:**

12 1. This section has been revised to make clear that a person
13 using an electronic agent is responsible for the results obtained
14 by setting the electronic agent in motion, and will be deemed to
15 have signed any such record.

16 2. This section extends signing to the electronic agent,
17 automated context. Its purpose is to establish that by
18 programming an electronic agent, a party assumes responsibility
19 for electronic records and operations "executed" by the program.
20 While the electronic agent may or may not execute a symbol
21 representing an electronic signature (i.e., with present human
22 intent to authenticate the electronic record), the party
23 programming the electronic agent has indicated its authentication
24 of records and operations produced by the electronic agent within
25 the parameters set by the programming. Accordingly, the party
26 should be bound and deemed to have signed the records of the
27 electronic agent.

28 **PART 4**

29 **ELECTRONIC CONTRACTS AND COMMUNICATIONS**

30 **SECTION 401. FORMATION AND VALIDITY.**

31 (a) Unless otherwise agreed, ~~if~~ an electronic record is
32 used in the formation of a contract, the contract may not be
33 denied legal effect, validity, or enforceability solely because

1 ~~on the sole ground that an electronic record was used for that~~
2 ~~purpose.~~

3 ~~(b) Operations of electronic agents which confirm the~~
4 ~~existence of a contract or signify agreement may form a contract~~
5 ~~even if no individual was aware of or reviewed the operations.~~

6 (b) In an automated transaction, the following rules
7 apply:

8 (1) A contract may be formed by the interaction of two
9 electronic agents. A contract is formed if the interaction
10 results in ~~both~~ the electronic agents engaging in operations that
11 confirm the existence of a contract or indicate signify
12 agreement, such as by engaging in performing the contract,
13 ordering or instructing performance, accepting performance, or
14 making a record of the existence of a contract.

15 (2) A contract may be formed by the interaction of an
16 electronic agent and an individual. A contract is formed by such
17 interaction if ~~(A) the individual has reason to know (i) that the~~
18 ~~individual is dealing with an electronic agent and (ii) the~~
19 ~~limitations on the ability of the electronic agent to react to~~
20 ~~contemporaneous expressions by the individual and (B) the~~
21 individual performs actions that the individual knows or
22 reasonably should know will cause the electronic agent to
23 complete the transaction, or performance or permit further use,
24 or that which are clearly indicated as constituting acceptance,
25 regardless of other expressions or actions by the individual to

1 which the individual cannot reasonably expect the electronic
2 agent to react.

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

5 (A) terms of the parties' agreement ~~(including terms~~
6 ~~with respect to which either party has manifested assent)~~, i

7 (b) terms that the electronic agent could take into
8 account, i and,

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

11 (4) A person is bound by the terms and agreements
12 resulting from the operations of its electronic agent even if no
13 individual was aware of or reviewed the electronic agent's
14 actions or the resulting terms and agreements.

15 ~~(c)~~ If an electronic record initiated by a party or an
16 electronic agent evokes an electronic record in response and the
17 records reflect an intent to be bound, a contract is formed
18 ~~exists when:~~

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

21 (2) if the response consists of electronically
22 performing the requested consideration in whole or in part, when
23 the requested consideration, to be performed electronically, is
24 received, unless the originating record prohibited that form of
25 response.

26 **Source:** Article 2B Draft Section 2B-204; Uncitral Model Article
27 11.

1 **Committee Vote:** To delete the concept of manifestation of assent
2 from Subsection (b)(3) (former subsection (c)(3)) Committee 6 Yes
3 - 0 No Observers 15 Yes - 0 No

4 **Reporter's Note:**

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

14 2. Subsection (b) has been revised for clarity and to more
15 closely track the revision in Article 2B. The subsection
16 addresses those transactions not involving human review by one or
17 both parties and provides rules to expressly validate contract
18 formation when electronic agents are involved. It sets forth the
19 circumstances under which formation will occur in a fully
20 automated transaction and under an automated transaction where
21 one party is an individual. Former subsection (b) has been moved
22 as part of this new subsection to confirm that a person is bound
23 by the actions of its electronic agents in these types of
24 transactions.

25 3. Subsection (b)(2) has been revised to eliminate the
26 requirements that an individual dealing with an electronic agent
27 know both that it is dealing with an electronic agent and the
28 limitations on the agent's ability to respond to the individual.
29 This revision differs from the provision of Article 2B-204 which
30 still retains these requirements.

31 As noted in a number of comments at the January meeting,
32 whether one knows that one is dealing with an electronic agent
33 should be irrelevant, so long as the individual proceeds with
34 actions it knows or reasonably should know will result in
35 accomplishment of the ends desired. Concerns previously
36 expressed by observers that individuals may not know what
37 contemporaneous statements made by the individual would be given
38 effect because of the possibility of contemporaneous or
39 subsequent human review, have been addressed by limiting those
40 actions of the individual which may result in a contract to those
41 which the individual would reasonably expect to result in a
42 contract. This will provide the party employing an electronic
43 agent with an incentive to make clear the parameters of the
44 agent's ability to respond. If the party employing the
45 electronic agent provides such information, the individual's act
46 of proceeding on the basis of contemporaneous actions or
47 expressions not within the parameters of the agent would be
48 unreasonable and such actions and expressions could not be the
49 basis for contract formation.

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

9 **SECTION 402. TIME AND PLACE OF SENDING AND RECEIPT.**

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

15 (b) Unless otherwise agreed between the sender and the
16 recipient, an electronic record is received when the electronic
17 record enters an information processing system from which the
18 recipient is able to retrieve electronic records, in a form
19 capable of being processed by that system, and the recipient uses
20 or has designated that system for the purpose of receiving such
21 electronic records or information. ~~In addition, a~~An electronic
22 record is also received when ~~it comes to the attention of the~~
23 recipient acquires knowledge of it.

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

28 (d) Unless otherwise agreed between the sender and the
29 recipient, an electronic record is deemed to be sent from where
30 the sender has its place of business and is deemed to be received

1 where the recipient has its place of business. For the purposes
2 of this subsection:

3 (1) if the sender or recipient has more than one place
4 of business, the place of business is that which has the closest
5 relationship to the underlying transaction or, if there is no
6 underlying transaction, the principal place of business; and

7 (2) if the sender or the recipient does not have a
8 place of business, the place of business is the recipient's
9 habitual residence.

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

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

15 **Reporter's Note:**

16 1. This section provides default rules regarding when an
17 electronic record is sent and when and where an electronic record
18 is received. As with acknowledgments of receipt under Section
19 403, this section does not address the efficacy of the record
20 that is received. That is, whether a record is unintelligible or
21 unusable by a recipient is a separate issue from whether that
22 record was received.

23 2. Subsection (b) is from the former definition of received in
24 the August draft. It provides simply that when a record enters
25 the system which the recipient has designated or uses and to
26 which it has access, in a form capable of being processed by that
27 system, it is received. Unless the parties have agreed
28 otherwise, entry into any system to which the recipient has
29 access will suffice. By keying receipt to a system which is
30 accessible by the recipient, the issue of leaving messages with a
31 server or other service is removed. However, the issue of how
32 the sender proves the time of receipt is not resolved by this
33 section. The last sentence provides the ultimate fallback by
34 providing that in all events a record is received when the
35 recipient has knowledge of it.

36 3. Subsections (c) and (d) provide default rules for
37 determining where a record will be considered to have been
38 received. The focus is on the place of business of the recipient

1 and not the physical location of the information processing
2 system. As noted in paragraph 100 of the commentary to the
3 Uncitral Model Law
4

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

11 Accordingly, where the place of sending or receipt is an issue,
12 the relevant location should be the location of the sender or
13 recipient and not the location of the information processing
14 system.
15

16 4. Subsection (e) rejects the mailbox rule and provides that
17 electronic records are effective on receipt. This approach is
18 consistent with Article 4A and, as to electronic records, Article
19 2B.

20 **SECTION 403. ELECTRONIC ACKNOWLEDGMENT OF RECEIPT.**

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

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

30 (2) If the sender ~~requests electronic acknowledgment~~
31 ~~but does not state~~ indicate that the record is conditional on
32 electronic acknowledgment, ~~and does not~~ specify a time for
33 receipt, and electronic acknowledgment is not received within a
34 reasonable time after the record is sent, the sender, upon
35 ~~notifying~~ ce to the other party, may: ~~either~~

1 (A) treat the record as ~~having expired~~ no longer
2 effective; or

3 (B) specify a further reasonable time within
4 which electronic acknowledgment must be received and, if
5 acknowledgement is not received within that time, or the message
6 will be treated the record as having expired no longer effective.
7 ~~If electronic acknowledgment is not received within that~~
8 ~~additional time, the sender may treat the record as not having~~
9 ~~binding effect.~~

10 (3) If the sender ~~requests electronic acknowledgment~~
11 ~~and~~ specifies a time for receipt, if and receipt does not occur
12 within that time, the sender may treat the record as no longer
13 effective ~~having expired.~~

14 (b) Receipt of electronic acknowledgment ~~establishes~~
15 creates a presumption that the record was received but, in
16 itself, does not establish that the content sent corresponds to
17 the content received.

18 **Source:** Article 2B Draft Section 2B-120(b)&(c); Uncitral Model
19 Article 14.

20 **Notes to This Draft.** Edited for clarity and to more closely
21 track Article 2B.

22 **Reporter's Note:** This section deals with functional
23 acknowledgments as described in the ABA Model Trading Partner
24 Agreement. The purpose of such functional acknowledgments is to
25 confirm receipt, and not necessarily to result in legal
26 consequences flowing from the acknowledgment.

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

32 As noted in subsection (b) the only effect of a functional
33 acknowledgment is to establish receipt. The acknowledgment alone
34 does not affect questions regarding the binding effect of the
35 acknowledgment nor the content, accuracy, time of receipt or

1 other issues regarding the legal efficacy of the record or
2 acknowledgment.

3 **SECTION 404. ADMISSIBILITY INTO EVIDENCE.**

4 (a) In any legal proceeding, the rules of evidence ~~must~~ may
5 not be applied to deny the admissibility in evidence of an
6 electronic record or electronic signature:

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

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

11 (b) In assessing the evidentiary weight of an electronic
12 record or electronic signature, the trier of fact shall consider
13 the manner in which the electronic record or electronic signature
14 was generated, stored, communicated, or retrieved, the
15 reliability of the manner in which the integrity of the
16 electronic record or electronic signature was maintained, the
17 manner in which its originator was identified or the electronic
18 record was signed, and any other relevant ~~information or~~
19 circumstances.

20 **Source:** UETA Section 206 (August Draft); Uncitral Model Article
21 9; Illinois Model Section 205.

22 **Reporter's Note:** Like sections 201(a) and 301(a), subsection
23 (a)(1) prevents the nonrecognition of electronic records and
24 signatures solely on the ground of the media in which information
25 is presented. Subsection (a)(2) also precludes inadmissibility on
26 the ground an electronic record is not an original.

27 Nothing in this section relieves a party from establishing
28 the necessary foundation for the admission of an electronic
29 record. Subsection (b) gives guidance to the trier of fact in
30 according weight to otherwise admissible electronic evidence.
31

1 **SECTION 405. TRANSFERABLE RECORDS.** If the identity of the
2 ~~rightful holder of person entitled to enforce~~ a transferable
3 record can be reliably determined from the record itself or from
4 a method employed for recording, registering, or otherwise
5 evidencing the transfer of interests in such records, the
6 ~~rightful holder of person entitled to enforce~~ the record is
7 ~~considered~~ deemed to be in possession of the record.

8 **Source:** Oklahoma Model Section III.B.2.

9 **Reporter's Note:** This section has been retained for discussion
10 by the Drafting Committee on whether such documents should be
11 covered by this Act.

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

19 PART 5

20 GOVERNMENTAL ELECTRONIC RECORDS

21 **SECTION 501. USE CREATION AND RETENTION OF ELECTRONIC RECORDS AND** 22 **CONVERSION OF WRITTEN RECORDS BY STATE GOVERNMENTAL AGENCIES.**

23 ~~(a) — [Except where Unless expressly prohibited by statute,]~~
24 ~~Every~~ Each ~~state~~ governmental agency ~~may~~ shall determine if, and
25 the extent to which, it will create and retain electronic records
26 ~~in place~~ instead of written records and ~~may~~ convert written
27 records to electronic records. [The [designated state officer]
28 shall ~~issue~~ adopt rules governing the disposition of written
29 records after conversion to electronic records.]

30 **Source:** Massachusetts Electronic Records and Signatures Act
31 Section 3 (Draft - November 4, 1997)

32 **Reporter's Notes:** See Notes following Section 504.

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

3 (~~a~~b) ~~Any state~~ [Except where expressly prohibited by
4 statute] Each governmental agency shall determine if, and the
5 extent to which, it will send and receive electronic records and
6 electronic signatures to and from other persons, and otherwise
7 create, use, store and rely upon electronic records and
8 electronic signatures. ~~that accepts the filing of records or~~
9 ~~requires that records be created or retained by any person may~~
10 ~~authorize the filing, creation, or retention of records in the~~
11 ~~form of electronic records [except where expressly prohibited by~~
12 ~~statute].—~~

13 (~~b~~c) In any case governed by subsection (a) ~~or (b)~~, the
14 ~~state~~ governmental agency, by appropriate regulation giving due
15 consideration to security, [may] [shall] specify:

16 (1) the manner and format in which the electronic
17 records must be ~~filed~~, created, sent, received and stored ~~or~~
18 ~~retained~~;

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

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

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

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

11 ~~(d) In establishing regulations under subsection (c) state~~
12 ~~governmental agencies shall give due regard to regulations~~
13 ~~implemented by other state governmental agencies, other states~~
14 ~~and the federal government for the purpose of avoiding, to the~~
15 ~~greatest extent possible, conflicting regulations which would~~
16 ~~impede commerce and the implementation of electronic~~
17 ~~transactions.~~

18 ~~(de) Nothing in t~~This [Act] may be construed to does not
19 require any state governmental agency to use or permit the use of
20 electronic records or electronic signatures.

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

23 **Reporter's Note:** See Notes following Section 504.

24 **SECTION 503. [DESIGNATED STATE OFFICER] TO ADOPT STATE STANDARDS.**

25 The [designated state officer] may adopt regulations setting
26 forth rules, standards, procedures and policies for the use of
27 electronic records and electronic signatures by governmental

1 agencies. Where appropriate, such regulations shall specify
2 differing levels of standards from which implementing
3 governmental agencies can choose in implementing the most
4 appropriate standard for a particular application.

5 **Source:** Illinois Model Section 802(a).

6 **Reporter's Note:** See Notes following Section 504.

7 **SECTION 504. INTEROPERABILITY.** To the extent practicable under
8 the circumstances, regulations adopted by [designated state
9 officer] or a governmental agency relating to the use of
10 electronic records or electronic signatures shall be drafted in a
11 manner designed to encourage and promote consistency and
12 interoperability with similar requirements adopted by
13 governmental agencies of other states and the federal government.

14 **Source:** Illinois Model Section 803.

15 **Reporter's Notes to Part 5.** This Part addresses the expanded
16 scope of this Act.

17 1. Section 501 is derived from former subsection 501(a) and
18 authorizes state agencies to use electronic records and
19 electronic signatures generally for intra-governmental purposes,
20 and to convert written records and manual signatures to
21 electronic records and electronic signatures. By its terms it
22 leaves the decision to use electronic records or convert written
23 records and signatures to the governmental agency. It also
24 authorizes the destruction of written records after conversion to
25 electronic form. In this regard, the bracketed language requires
26 the appropriate state officer to issue regulations governing such
27 conversions.

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

34 2. Subsection 502(c) requires governmental agencies, in
35 adopting regulations for the use of electronic records and
36 signatures to conform to standards established by the designated

1 state officer under Section 503. The question here is whether
2 the state agencies should be required, or merely permitted, to
3 promulgate such regulations before accepting electronic records?

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

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

1 **PART 6**

2 **MISCELLANEOUS PROVISIONS**

3 **SECTION 601. SEVERABILITY CLAUSE.** If a provision of this
4 [Act], or an application thereof to any person or circumstance,
5 is held invalid, the invalidity does not affect other provisions
6 or applications of the [Act] that can be given effect without the
7 invalid provision or application, and to this end the provisions
8 of this [Act] are severable.

9 **Source:** Article 1 Draft Section 1-106.

10 **SECTION 602. EFFECTIVE DATE.**

11 **Source:**

12 **SECTION 603. SAVINGS AND TRANSITIONAL PROVISIONS.**

13 **Source:**