

D R A F T
FOR DISCUSSION ONLY

UNIFORM ELECTRONIC TRANSACTIONS ACT

NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS

JANUARY 29, 1999

UNIFORM ELECTRONIC TRANSACTIONS ACT

With Reporter's Notes

Copyright© 1999
By
NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS

The ideas and conclusions set forth in this draft, including the proposed statutory language and any comments or reporter's notes, have not been passed upon by the National Conference of Commissioners on Uniform State Laws or the Drafting Committee. They do not necessarily reflect the views of the Conference and its Commissioners and the Drafting Committee and its Members and Reporters. Proposed statutory language may not be used to ascertain the intent or meaning of any promulgated final statutory proposal.

DRAFTING COMMITTEE ON

UNIFORM ELECTRONIC TRANSACTIONS ACT

PATRICIA BRUMFIELD FRY, University of North Dakota, School of Law, P.O. Box 9003,
Grand Forks, ND 58201, Chair

STEPHEN Y. CHOW, One Beacon Street, 30th Floor, Boston, MA 02108

KENNETH W. ELLIOTT, Suite 630, 119 N. Robinson Avenue, Oklahoma City, OK 73102

HENRY DEEB GABRIEL, JR., Loyola University, School of Law, 526 Pine Street, New
Orleans, LA 70118

BION M. GREGORY, Office of Legislative Counsel, State Capitol, Suite 3021, Sacramento, CA
95814-4996

JOSEPH P. MAZUREK, Office of Attorney General, P.O. Box 201401, 215 N. Sanders, Helena,
MT 59620

PAMELA MEADE SARGENT, P.O. Box 846, Abingdon, VA 24212

D. BENJAMIN BEARD, University of Idaho, School of Law, 6th and Rayburn Streets, Moscow,
ID 83844-2321, Reporter

EX OFFICIO

GENE N. LEBRUN, P.O. Box 8250, 9th Floor, 909 St. Joseph Street, Rapid City, SD 57709,
President

HENRY M. KITTLESON, P.O. Box 32092, 92 Lake Wire Drive, Lakeland, FL 33802-2092,
Division Chair

AMERICAN BAR ASSOCIATION ADVISORS

C. ROBERT BEATTIE, 150 S. 5th Street, Suite 3500, Minneapolis, MN 55402, Business Law
Section

AMELIA H. BOSS, Temple University, School of Law, 1719 N. Broad Street, Philadelphia, PA
19122, Advisor

THOMAS J. SMEDINGHOFF, 500 W. Madison Street, 40th Floor, Chicago, IL 60661-2511,
Science and Technology Section

EXECUTIVE DIRECTOR

FRED H. MILLER, University of Oklahoma, College of Law, 300 Timberdell Road, Norman,
OK 73019, Executive Director

WILLIAM J. PIERCE, 1505 Roxbury Road, Ann Arbor, MI 48104, Executive Director
Emeritus

Copies of this Act may be obtained from:
NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS
211 E. Ontario Street, Suite 1300
Chicago, Illinois 60611
312/915-0195

TABLE OF DISPOSITION OF SECTIONS IN SEPTEMBER 18, 1998 DRAFT

September 18, 1998 Draft Section	January 25, 1999 Draft Section
101.....	101
102.....	102
103.....	103(a)
104(a).....	103(b)
104(b).....	103(c)
104(c).....	103(b)(7)
104(d).....	108
104(e).....	103(d)
105.....	104
106.....	105
107.....	Deleted
108.....	Deleted
109.....	Deleted
110.....	107
201(a).....	106(a)
201(b).....	106(c)
201(c).....	106(e)
202.....	109
203.....	110
204.....	116(a and d)
205(a).....	113(a and e)
205(b).....	Deleted
206.....	113(b, c, d, and f)
301(a).....	106(a)
301(b).....	106(d)
301(c).....	106(e)
302.....	111(a and c)
303(a).....	116(b)
303(b).....	111(b)
304.....	112
401(a).....	116(c)
401(b).....	115
401(c).....	106(b)
402.....	117(a-e)
403(a).....	Deleted
403(b).....	117(f)
404.....	114
405.....	118
501.....	201
502.....	202
503.....	Deleted
504.....	203

UNIFORM ELECTRONIC TRANSACTIONS ACT

TABLE OF CONTENTS

PART 1

~~GENERAL PROVISIONS~~

NON-GOVERNMENTAL RECORDS AND SIGNATURES

SECTION 101. SHORT TITLE.

SECTION 102. DEFINITIONS.

SECTION 103. SCOPE.

~~**SECTION 104. SCOPE - EXCLUSIONS AND LIMITATIONS.**~~

SECTION 104. VARIATION BY AGREEMENT.

SECTION ~~106~~ 105. APPLICATION AND CONSTRUCTION.

~~SECTION 107. MANIFESTING ASSENT.~~

~~SECTION 108. OPPORTUNITY TO REVIEW.~~

~~SECTION 109. DETERMINATION OF REASONABLE SECURITY PROCEDURE.~~

**SECTION ~~201~~ 106. LEGAL RECOGNITION OF ELECTRONIC RECORDS,
ELECTRONIC SIGNATURES AND ELECTRONIC CONTRACTS.**

SECTION 107. EFFECT OF REQUIRING UNREASONABLE SECURITY PROCEDURE.

SECTION 108. PROVISION OF INFORMATION IN WRITING.

~~PART 2~~

~~ELECTRONIC RECORDS~~

SECTION 202 109. ATTRIBUTION OF ELECTRONIC RECORD TO PARTY.

SECTION 203 110. DETECTION OF CHANGES AND ERRORS.

~~SECTION 204 INADVERTENT ERROR.~~

SECTION 302 111. EFFECT OF ELECTRONIC SIGNATURES.

~~SECTION 303 OPERATIONS OF ELECTRONIC DEVICES.~~

SECTION 304 112. NOTARIZATION AND ACKNOWLEDGMENT.

~~SECTION 205 ORIGINALS - INFORMATION ACCURACY.~~

SECTION 404 113. RETENTION OF ELECTRONIC RECORDS; ORIGINALS.

SECTION 114. ADMISSIBILITY INTO EVIDENCE.

SECTION 115. FORMATION OF CONTRACT AND VALIDITY.

SECTION 116. OPERATIONS OF ELECTRONIC AGENT; AUTOMATED TRANSACTIONS.

SECTION 402.117. TIME AND PLACE OF SENDING AND RECEIPT.

~~SECTION 403. ELECTRONIC ACKNOWLEDGMENT OF RECEIPT.~~

SECTION 405 118. CONTROL OF TRANSFERABLE RECORDS.

~~—————PART 3~~
~~—————ELECTRONIC SIGNATURES~~

~~SECTION 301. LEGAL RECOGNITION OF ELECTRONIC SIGNATURES.~~
~~SECTION 302. EFFECT OF ELECTRONIC SIGNATURES.~~
~~SECTION 303. OPERATIONS OF ELECTRONIC DEVICES.~~
~~SECTION 304. NOTARIZATION AND ACKNOWLEDGMENT.~~

~~—————PART 4~~
~~—————ELECTRONIC CONTRACTS AND COMMUNICATIONS~~

~~SECTION 401. FORMATION AND VALIDITY.~~
~~SECTION 402. TIME AND PLACE OF SENDING AND RECEIPT.~~
~~SECTION 403. ELECTRONIC ACKNOWLEDGMENT OF RECEIPT.~~
~~SECTION 404. ADMISSIBILITY INTO EVIDENCE.~~
~~SECTION 405. TRANSFERABLE RECORDS.~~

PART 5 2
GOVERNMENTAL ELECTRONIC RECORDS

~~SECTION 501~~ **201. CREATION AND RETENTION OF ELECTRONIC
RECORDS AND CONVERSION OF WRITTEN RECORDS BY
GOVERNMENTAL AGENCIES.**
~~SECTION 502~~ **202. RECEIPT AND DISTRIBUTION OF ELECTRONIC
RECORDS BY GOVERNMENTAL AGENCIES.**
~~SECTION 503~~ **203. [DESIGNATED STATE OFFICER] TO ADOPT STATE
STANDARDS.**
~~SECTION 504~~ **203. INTEROPERABILITY.**

PART 6 3
MISCELLANEOUS PROVISIONS

~~SECTION 601~~ **301. SEVERABILITY.**
~~SECTION 602~~ **302. EFFECTIVE DATE.**
~~SECTION 603~~ **303. SAVINGS AND TRANSITIONAL PROVISIONS.**

1 **PART 1**

2 **GENERAL PROVISIONS**

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

5 **SECTION 102. DEFINITIONS.**

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

7 (1) "Agreement" means the bargain of the parties in fact as found in their
8 language or inferred from other circumstances, and rules, regulations, and procedures
9 given the effect of agreements under rules of law otherwise applicable to a particular
10 transaction. [Whether an agreement has legal consequences is determined by this [Act],
11 if applicable, or otherwise by other applicable rules of law.]

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

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

20 (4) "Consumer" means an individual involved in a transaction primarily
21 for personal, family, or household purposes.

1 (5) "Consumer transaction" means a transaction in which a consumer is
2 involved.

3 (46) "Contract" means the total legal obligation resulting from the parties'
4 agreement as affected by this [Act] and other applicable rules of law.

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

7 (68) "Electronic agent device" means a computer program, ~~or other~~
8 electronic, ~~or other~~ automated means ~~configured and enabled by a person used~~ to initiate
9 or respond to electronic records or performances in whole or in part without review by an
10 individual.

11 (79) "Electronic record" means a record created, stored, generated,
12 received, or communicated by electronic means.

13 (810) "Electronic signature" means a signature in electronic form,
14 attached to or logically associated with an electronic record.

15 (911) " Governmental agency" means an executive[, legislative, or
16 judicial] agency, department, board, commission, authority, institution, or instrumentality
17 of ~~this~~ the federal government or of a state or of any county, municipality, ~~or other~~
18 political subdivision of ~~this~~ a state.

19 (1012) "Information" means data, text, images, sounds, codes, computer
20 programs, software, databases, or the like.

1 (13) "Information processing system" means an electronic system for
2 creating, generating, sending, receiving, storing, displaying, or ~~otherwise~~ processing
3 information.

4 (14) "Informational content" means information that ~~in its ordinary use~~
5 is intended to be communicated to or perceived by ~~a person~~ an individual in the ordinary
6 use of the information.

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

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

10 (15) "Person" means an individual, corporation, business trust, estate,
11 trust, partnership, limited liability company, association, joint venture, two or more
12 persons having a joint or common interest, governmental agency, ~~government~~,
13 ~~governmental subdivision, agency, instrumentality~~, or public corporation, or any other
14 legal or commercial entity.

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

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

1 (18) "Security procedure," means a procedure ~~or method, [established by~~
2 ~~law or agreement, or knowingly adopted by each party,]~~ employed for the purpose of
3 verifying that an electronic signature, record, or performance is that of a specific person
4 or for detecting changes or errors in the informational content of an electronic record.
5 The term includes a procedure that requires the use of algorithms or other codes,
6 identifying words or numbers, encryption, callback or other acknowledgment procedures;
7 ~~or any other procedures that are reasonable under the circumstances.~~

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

9 (20) "Signature" means an identifying symbol, sound, or process,~~or~~
10 ~~encryption of a record in whole or in part, that is attached to or associated with a record~~
11 and executed or adopted by a person to associate the person with the record, ~~as part of a~~
12 ~~record.~~

13 (21) ~~"Term" means that portion of an agreement which relates to a~~
14 ~~particular matter.~~

15 _____(2221) "Transaction" means an action or set of actions occurring between
16 two or more persons relating to the conduct of business or governmental affairs. ~~taken by~~
17 ~~a person which relate to or involve another person or persons.~~

18 (252) "Transferable record" means a record, other than a writing, that
19 would be a note under [Article 3 of the Uniform Commercial Code], an instrument or
20 chattel paper under [Article 9 of the Uniform Commercial Code], or a document of title
21 under [Article 1 of the Uniform Commercial Code], if the record were in writing.

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

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

~~—————"Inadvertent error". Section 204~~

~~—————"Requiring party". Section 110~~

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

Reporter's Note: The qualification to the introductory clause has been deleted based on comments from the Committee on Style that it is unnecessary and creates ambiguity.

1. "Agreement"

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)

Revised to conform to language in Article 2B.

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, 1997 Draft was taken from the most recent revision to Article 1.

At the January, 1998 Meeting, the Committee more specifically defined the policy guiding this Act: the Act is a procedural act providing for the means to effectuate transactions accomplished via an electronic medium, and, unless absolutely necessary because of the unique circumstances of the electronic medium, the Act should leave all questions of substantive law to law outside this Act. In light of this principle the prior references to usage evidence as informing the content of an agreement was considered substantive, and therefore, best left to other law outside this Act.

The need for a definition of agreement arises because the existence of a security procedure often depends on the agreement of the parties. However, the facts and

1 evidence which establish an agreement are left to other law, e.g., the Uniform
2 Commercial Code, common law, etc.

3 Whether the parties have reached an agreement is determined by their express
4 language and surrounding circumstances. The Restatement of Contracts §3 provides that
5 "An agreement is a manifestation of mutual assent on the part of two or more
6 persons. A bargain is an agreement to exchange promises or to exchange a
7 promise for a performance or to exchange performances."

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

11 The provisions in the last clause of the first sentence are intended to include
12 circumstances where the law deems agreements to exist as a matter of a rule, regulation
13 or otherwise. For example, Article 4 (Section 4-103(b)) provides that Federal Reserve
14 regulations and operating circulars and clearinghouse rules have the effect of agreements.
15 Such agreements by law are properly included in the definition in this Act.

16 The existence and content of an agreement under this Act are determined by the
17 parties' language and surrounding circumstances. The relevant surrounding
18 circumstances and the context of the transaction will inform the precise terms of any
19 agreement. The second sentence of this definition makes clear that the substantive law
20 applicable to an electronic transaction effectuated by this Act must be applied to
21 determine those circumstances relevant in establishing the precise scope and meaning of
22 the parties' agreement. **THE STYLE COMMITTEE VIEWS THE PROVISION AS**
23 **SUBSTANTIVE AND CONTENDS THAT IT SHOULD NOT BE INCLUDED IN**
24 **THE DEFINITION.** Considering the source of this provision is the UCC, which has a
25 40-50 year history of construction, **THE PROVISION HAS BEEN RETAINED FOR**
26 **DISCUSSION BY THE DRAFTING COMMITTEE AT ITS NEXT MEETING.**

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

30 2. "Automated Transaction."

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

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

38 As with electronic agents, this definition addresses the circumstance where
39 electronic records may result in action or performance by a party although no human
40 review of the electronic records is anticipated. Section 116 provides specific contract
41 formation rules where one or both parties do not review the electronic records.

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

3 4. **"Consumer."** This definition has been added in order to provide a means to limit the
4 effect of Sections 107 and 108, should the Drafting Committee so choose.

5 5. **"Consumer transaction."** This definition has been added in order to provide a means
6 to limit the effect of Sections 107 and 108, should the Drafting Committee so choose.

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

11
12 7. **"Electronic agent."** This Act used the term "electronic device" (rather than
13 "electronic agent" used in Article 2B) in order to avoid connotations of agency.
14 However, in Article 2B and in other contexts the term "electronic agent" has come to be
15 recognized as a near term of art. The term "electronic device" has not been widely hailed
16 as a significant improvement. Accordingly, the Chair and Reporter of UETA agreed in
17 the coordination meeting to adopt "electronic agent" in order to be consistent with Article
18 2B. (Article 2B will adopt the language in the definition and the only point of difference
19 will be the phrase "in whole or in part" after the word "performances" which will not be
20 included in Article 2B.) Comments made at UETA Drafting Committee meetings from
21 members of the Committee and observers highlight that the key aspect of this term is its
22 function as a tool of a party. As the term "electronic agent" has come to be recognized, it
23 is limited to the tool function.

24 The definition has been revised to reflect comments that, for purposes of the
25 definition, it is irrelevant who employs the agent. Rather the definition establishes that an
26 electronic agent is a machine. The effect on the party using the agent is addressed in the
27 operative provisions of the Act (e.g., Section 116(b))

28 An electronic agent, such as a computer program or other automated means
29 employed by a person, is a tool of that person. As a general rule, the employer of a tool is
30 responsible for the results obtained by the use of that tool since the tool has no
31 independent volition of its own. However, an electronic agent by definition is capable,
32 within the parameters of its programming, of initiating, responding or interacting with
33 other parties or their electronic agents once it has been activated by a party, without
34 further attention of that party. This Act (Section 116(b)) provides that a person is
35 responsible for actions taken and accomplished through electronic agents in the absence
36 of human intervention.

37 While this Act proceeds on the paradigm that an electronic agent is capable of
38 performing only within the technical strictures of its preset programming, it is
39 conceivable that, within the useful life of this Act, electronic agents may be created with
40 the ability to act autonomously, and not just automatically. That is, through
41 developments in artificial intelligence, a computer may be able to "learn through

1 experience, modify the instructions in their own programs, and even devise new
2 instructions." Allen and Widdison, "Can Computers Make Contracts?" 9 Harv. J.L.&Tech
3 25 (Winter, 1996). If such developments occur, courts may construe the definition of
4 electronic agent accordingly, in order to recognize such new capabilities.

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

10 Electronic means for creating, storing, generating, receiving or communicating
11 electronic records include information processing systems, computer equipment and
12 programs, electronic data interchange, electronic mail, or voice mail, facsimile, telex,
13 telecopying, scanning, and similar technologies.

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

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

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

29 **10. "Governmental agency."**

30 **Committee Vote:** To include legislative and judicial agencies - 3 Yea - 0 Nay (October,
31 1998)

32 This definition is important in the context of Part 2. The reference to legislative and
33 judicial agencies has been included per the vote of the Committee in Rapid City. The
34 definition has also been expanded to be a generic description unrelated to any particular
35 State. This was necessitated by the use of the term in Section 203 on Interoperability.
36 Where governmental agencies of the enacting state are relevant this has been clarified in
37 the operative provisions.

38 **11. "Information processing system."** This term is used in Section 118 regarding the
39 time and place of receipt of an electronic record. It has been revised to conform with
40 Article 2B.

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

8 13. **"Notify."** This definition has been deleted since there are no longer any references in
9 the Act.

10 14. **"Organization."** This definition has been deleted since there are no longer any
11 references in the Act.

12 15. **"Person."** This definition has been clarified by incorporating the definition of
13 governmental agency.

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

15 17. **"Rule of Law."** The definition is drafted broadly. **IT HAS BEEN BRACKETED**
16 **IN RECOGNITION OF THE STYLE COMMITTEE'S RECOMMENDATION**
17 **THAT IT BE DELETED AND THE UNDEFINED TERM "LAW" BE**
18 **SUBSTITUTED. IT HAS BEEN RETAINED FOR DRAFTING COMMITTEE**
19 **CONSIDERATION.**

20 18. **"Security procedure."** It was suggested at the Annual Meeting that the way in which
21 a security procedure becomes applicable should be referenced in the substantive rule and
22 not set forth as part of the definition. Accordingly, this clause has been deleted and the
23 definition revised for clarity and to more closely parallel Article 2B.

24 The only provision in the Act addressing the effect of security procedures in a
25 given transaction is Section 107.

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

32 19. **Signature."** As part of the coordination meeting regarding Article 2B, the
33 differences between the definition of authentication in 2B (and revised Article 9) and
34 UETA were noted. It was suggested that the UETA consider adopting a definition of
35 "signature" which deferred to the applicable definition of signature provided by the
36 substantive law applicable to a given transaction or in the alternative, that UETA not
37 define the term. **THIS IDEA IS NOTED FOR CONSIDERATION BY THE**
38 **COMMITTEE.**

1 At the September, 1997 Drafting Meeting, the consensus of the Committee and
2 observers was to go back to the definition of signature, and to delete the definition of
3 "authenticate." Given the purpose of this Act to equate electronic signatures with written
4 signatures, the sense was that retaining signature as the operative word would better
5 accomplish that purpose. However, the idea of fleshing out the concept of authenticate
6 present in the existing UCC definition of signature was thought to be wise. Therefore,
7 the definitional concepts set forth in the definition of authenticate in Article 2B were
8 carried into the definition of signature.

9 At the April 1998 meeting a good deal of discussion related to the propriety of
10 delineating the specific functions of a signature. The Committee deleted from former
11 Section 302 a provision establishing the specific effects of an electronic signature. The
12 one critical aspect of a signature that was recognized was its purpose of identifying a
13 person. Accordingly, the definition has been revised to reflect the principal function of a
14 signature as an identifying mark. In addition, some volition must attach to application of
15 a mark and this is noted by the requirement that the mark be "executed or adopted" by a
16 person. This draft also requires that the mark, etc, be executed or adopted for the purpose
17 of associating the person with the record, in order to distinguish a signature from a mere
18 autograph.

19 At the Annual Meeting it was suggested that an unrecorded statement over the
20 phone might qualify as a signature under this broadened definition. In order to address
21 this concern the definition now indicates that the symbol or sound must be attached to or
22 associated with the record. The effect of the signature is left to the underlying substantive
23 law in light of the facts and circumstances. See Section 111. In short, the definition here
24 reflects the bare minimum as to the function of a signature, with the substantive effect
25 being treated in Section 111 and the substantive law underlying the transaction.

26 20. **"Term."** This definition has been deleted since it is not used in the Act in any way
27 requiring definition.

28 21. **"Transaction."** This definition has been revised for clarity and specificity in light of
29 comments made at the October, 1998 meeting that it was too broad. Accordingly, it is
30 now limited to actions between people taken in the context of commercial or
31 governmental activities.

32 22. **"Transferable record."** This definition is necessary in the event the Drafting
33 Committee decides to retain Section 118. It has been revised to limit its applicability
34 solely to promissory notes under Article 3, consistent with the exclusion of "orders" from
35 the scope of the Act.

36 23. **"Writing."** This definition reflects the current UCC definition.

1 **SECTION 103. SCOPE.** (a) Except as otherwise provided in subsection (b) ~~104~~
2 , this [Act] applies to electronic records and electronic signatures that relate to any
3 transaction.

4 ~~**SECTION 104. SCOPE - EXCLUSIONS AND LIMITATIONS.**~~

5 (b a) This [Act] does not apply to electronic records and electronic signatures
6 related to a transaction to the extent that the transaction is governed by:

7 (1) a rules of law governing the creation and execution of wills and
8 codicils;

9 (2) a rules of law governing the creation and execution of ~~personal~~
10 testamentary trusts ~~created and executed in connection with wills and codicils;~~

11 (3) [Articles 4, 5, and 8 of the Uniform Commercial Code];

12 (4) [Article 4A of the Uniform Commercial Code except that the
13 requirement of a written agreement in the following sections may be satisfied with
14 electronic records and signatures:....]

15 (5) a rules of law governing the issuance, transfer, negotiation, or
16 enforcement of orders as defined in [Article 3 of the Uniform Commercial Code];
17 _____

18 (36) a rule of law which expressly authorizes the use of other than written
19 records or manual signatures in satisfaction of the rule ~~provides for the method and~~
20 ~~manner under which electronic records and electronic signatures may be used in~~
21 ~~satisfaction of the rule;~~ _____

_____ (47) [Other transactions identified by ETA Task Force on excluded transactions];

(8) [other transactions, if any, identified by State]; and

(5 9) Transactions specifically excluded by any governmental agency of this State under Part 2 5.

_____ (c b) In a statute, rule, or regulation containing a rule of law described in subparagraph (a b)(36), any express requirement elsewhere in that statute, rule, or regulation that a record be in writing ~~shall~~ is not be affected by this [Act] if the court determines that application of this [Act] would be contrary to the purpose of the requirement.

(d e) ~~Except as otherwise specifically provided in Subsection (d), This Act does not apply affect to a provision in a requirement in a rule of law relating to a specific mode of delivery or display of information.~~

_____ (d) If a rule of law requires a person to provide information in writing to another person that requirement is satisfied if the information is provided in an electronic record which is

_____ (1) ~~provided in an electronic record which is under the control of the person to which it is provided; and~~

_____ (2) ~~capable of retention for subsequent reference.~~ [Substance moved to section 108]

(e) A transaction subject to this [Act] is also subject to other applicable substantive rules of law, ~~which substantive~~ These rules of law must be construed

1 whenever reasonable as consistent with this [Act]. If ~~such a~~ this construction is
2 unreasonable, the ~~substantive~~ rule of law governs.

3 **Source:** UETA Sections 103 and 104 (Sept., 1998 Draft); Section 103 of Revised Draft
4 of Article 1.

5 **Committee Votes:**

6 1. In former Section 103:

7 a. To delete references to commercial and governmental transactions - Committee
8 4 Yes - 3 No (Chair broke tie) Observers 19 Yes - 1 No (Jan. 1998).

9 b. To incorporate supplemental principles as part of Scope section - Committee
10 Yes Unanimous Observers 12 Yes - 0 No (Jan. 1998).

11 c. To delete reference to supplemental principles (April 1998)

12 2. In former Section 104 to delete "repugnancy" language, and provide that Act will
13 apply except for specific exclusions. Committee 4 Yes - 1 No Observers 14 Yes - 1 No
14 (with a number of abstentions)(Jan. 1998)

15 **Reporter's Note to This Draft:**

16 1. Former Sections 103 and 104 have been combined into a single scope section per
17 comments of the Style Committee. Subsection (b) has been revised to make the scope
18 and exclusion provisions parallel in applicability to electronic records and electronic
19 signatures related to transactions.

20 2. The language in subsection (b)(2) has been revised for clarity. Use of the term
21 "testamentary trusts" is a known term of art.

22 3. The relationship of this Act to the Uniform Commercial Code remains, perhaps,
23 the most difficult question of scope. In the course of the revision projects of the last
24 decade developments with electronic media have been considered to a greater or lesser
25 degree in each of the revised Articles. The revisions of Articles 5 and 8 provide for
26 significant media neutrality and should not be affected by this Act.

27 Article 4A could be wholly excluded, with minimal effect. However, the level of
28 consideration of electronic media throughout the entire statute was not as thorough as
29 with Article 5 and Article 8. For example, the provisions for agreements regarding
30 commercially unreasonable security procedures must be in writing, and it is not clear that
31 such agreements could not as well be accomplished electronically. Determining which
32 sections are to be included within UETA will require care. The Reporter will prepare
33 such exceptions for the April meeting of the Committee, if the Committee determines that
34 this is the appropriate method for addressing Article 4A.

35 Although Article 4 specifically authorized electronic presentment and check
36 truncation, the check collection system remains predominantly paper based. Discussions
37 with representatives of the Federal Reserve have demonstrated significant concerns about
38 this Act having any impact on the current system of check collection. Accordingly, the
39 definition of, and provisions regarding, transferable records in Section 118 have been
40 limited to promissory note equivalents, and orders under Article 3 have been eliminated
41 from the Scope of this Act. Considering the highly regulated and largely closed nature of

1 the check collection system, exclusion of Article 4 from the Act seems a reasonable
2 approach.

3 The principal reason for retaining applicability of the UETA to the UCC relates to
4 the status of enactment for revised Articles 2, 2A, and 9 and proposed Article 2B. Upon
5 promulgation, these revisions will clearly fall within the exception in subparagraph (6)
6 because they will contain provisions for the use of electronic media, and under subsection
7 (c) will be unified entirety under which application of this Act to specific requirements
8 for writings will be contrary to the purpose of such requirements. However, until the
9 enactment of these revised Articles, the UETA has definite applicability in assuring that
10 sales, leases, licenses and secured transactions under the non-revised articles, will be
11 valid if done electronically. Accordingly, a broad exclusion for the UCC from the
12 UETA, as has been suggested by some, would be ill-advised.

13 In the same vein, other statutes where the use of electronic media was a conscious
14 part of the drafting process are also addressed by the interaction of subsection (b)(6) and
15 (c). Subsection (c) can be viewed as a limited "repugnancy" provision. That is, in a
16 statute which has specific provisions on electronic media, when the statute elsewhere
17 provides for a writing, this Act will not apply upon an affirmative finding by the court
18 that application of this Act would be contrary to the purpose of that writing requirement.

19 4. Subparagraph (8) preserves a space for individual states to exclude other
20 transactions which might be of particular concern in a given jurisdiction. Transactions
21 such as statutory powers of attorney, health powers, and perhaps even real estate
22 transactions might be excluded.

23 5. The exclusion in subsection (d) for rules of law calling for particular methods for
24 delivering or displaying information is intended to preserve such delivery/display
25 requirements regardless of the media used. If a notice must be displayed at a place of
26 business that requirement does not change simply because the notice may now be
27 electronic. However, the ability to properly display the notice, if it is only in electronic
28 form, may necessitate the use of paper. Similarly, if a rule of law requires delivery by US
29 postal service, this Act will not affect that requirement of the rule, and delivery by post of
30 a disc with the information on it would be required. This may in turn be subject to the
31 rule in Section 108 regarding provision of information in writing.

32 **Reporter's Note:**

33 1. The scope of the Act is limited to electronic records and electronic signatures.
34 The underlying premise of this section is that this Act applies to all electronic records and
35 signatures unless specifically excluded.

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

1 transactions was considered preferable to an attempt to redefine commercial and
2 governmental transactions.

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

10 4. The Task Force Report was completed at the end of September and was
11 extensively discussed at the October, 1998 meeting. Subsection (b) sets forth specific
12 exclusions and limitations to the coverage of this Act based on the Task Force Report, the
13 discussions at the October 1998 meeting and subsequent meetings and comments with
14 other interested parties.

15 **SECTION 104 ~~105~~. VARIATION BY AGREEMENT.**

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

18 (b) Except as otherwise provided in ~~subsections~~ 107 and 108 ~~(c) and (d)~~, as
19 between parties involved in generating, storing, sending, receiving, or otherwise
20 processing or using electronic records or electronic signatures, ~~the~~ provisions of this [Act]
21 may be varied by agreement. The presence in certain provisions of this [Act] of the words
22 "unless otherwise agreed", or words of similar import, does not imply that the effect of
23 other provisions may not be varied by agreement.

24 ~~(c) The determination of reasonableness in Section 109 may not be varied by~~
25 ~~agreement.~~

26 ~~(d) The effect of requiring an unreasonable security procedure stated in Section~~
27 ~~110 may not be varied by agreement.~~

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

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

5 **Committee Vote:** To move former subsection (c) to the end of subsection (b). Yea-3 Nay-
6 0 (October, 1998)

7 **Reporter's Note to this Draft:**

8 The only provisions of the Act which may not be varied by agreement are those in
9 Sections 107 and 108 regarding the effect of security procedures and the provision of
10 information in writing. In each case, the Drafting Committee may seek to limit the effect
11 of those sections to consumer transactions.

12 **Reporter's Note:**

13 1. Subsection (a) makes clear that this Act is intended to permit the use of electronic
14 media, but does not require any person to use electronic media. For example, if Chrysler
15 Corp. were to issue a recall of automobiles via its internet website, it would not be able to
16 rely on this Act to validate that notice in the case of a person who never logged on to the
17 website, or indeed, had no ability to do so. The provisions in Section 106 permitting a
18 person to establish reasonable forms for electronic records and signatures assumes a pre-
19 existing relationship between parties to a transaction, in which one party places reasonable
20 limits on the records and signatures, electronic or otherwise, which will be acceptable to it.
21 2. Given the principal purpose of this Act to validate and effectuate the use of electronic
22 media, it is important to preserve the ability of the parties to establish their own
23 requirements concerning the method of generating, storing and communicating with each
24 other. This Act affects substantive rules of contract law in very limited ways by giving
25 effect to actions done electronically. Even in those cases, the parties remain free to alter
26 the timing and effect of their communications.

27 **SECTION 105 ~~106~~. APPLICATION AND CONSTRUCTION.** This [Act]
28 must be construed ~~[liberally]~~ and applied consistently with reasonable practices under the
29 circumstances and to facilitate electronic transactions. ~~promote its purposes and policies.~~

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

31 **Committee Vote:** To delete "liberally" and substitute "facilitate electronic transactions".
32 Yea-3 Nay-0 (October, 1998)

33 **Reporter's Note to this Draft.** The Style Committee still believes that this section
34 smacks of a general purposes clause, creates ambiguity, and should be deleted.

35 **Reporter's Note:**

36 The purposes and policies of this Act are

1 a) to facilitate and promote commerce and governmental transactions by
2 validating and authorizing the use of electronic records and electronic signatures;
3 b) to eliminate barriers to electronic commerce and governmental
4 transactions resulting from uncertainties relating to writing and signature requirements;
5 c) to simplify, clarify and modernize the law governing commerce and
6 governmental transactions through the use of electronic means;
7 d) to permit the continued expansion of commercial and governmental
8 electronic practices through custom, usage and agreement of the parties;
9 e) to promote uniformity of the law among the states (and worldwide)
10 relating to the use of electronic and similar technological means of effecting and
11 performing commercial and governmental transactions;
12 f) to promote public confidence in the validity, integrity and reliability of
13 electronic commerce and governmental transactions; and
14 g) to promote the development of the legal and business infrastructure
15 necessary to implement electronic commerce and governmental transactions.

16 **SECTION ~~201~~ 106. LEGAL RECOGNITION OF ELECTRONIC**
17 **RECORDS, ELECTRONIC SIGNATURES AND ELECTRONIC CONTRACTS.**

18 (a) A record or signature may not be denied legal effect, ~~validity, or enforceability~~
19 solely because it is ~~an~~ in electronic form ~~record~~.

20 (b) A contract may not be denied legal effect, validity, or enforceability solely
21 because an electronic record was used in its formation.

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

24 (~~d~~) If a rule of law requires a signature, or provides consequences in the absence of
25 a signature, the rule of law is satisfied with respect to an electronic record if the electronic
26 record includes an electronic signature.

27 (~~c~~e) In ~~any~~ transaction, a person may establish reasonable requirements regarding
28 the type of records or signatures acceptable to it.

29 **Source:** UETA Sections 201, 301 and 401(a) (Sept. 1998 Draft).

1 **Reporter's Note to this Draft:**

2 1. Subsections (a and b) have been revised to delete the words “validity and
3 enforceability”. This makes the sections more parallel with Article 2B without altering the
4 meaning of the section.

5 2. This section reflects the significant reorganization from the September 1998 draft.
6 There are now only 18 sections regarding private electronic transactions and they all
7 appear in Part 1. Part 2 sets forth the provisions encouraging governmental agencies to
8 “go electronic.” This section combines the general effectiveness provisions for electronic
9 records and signatures and contracts taken from the noted sections of the prior draft.

10 3. At the September, 1998 meeting consideration of the annual meeting comment that
11 these rules should be stated in the positive rather than the negative confirmed that the rules
12 must be stated in the negative. This Act is only eliminating one ground for denying
13 validity to records, signatures and contracts. Accordingly it provides that the medium
14 cannot be the only ground for such a denial, and leaves to other law other grounds for
15 denying such validity.

16 **Reporter’s Note:**

17 1. Under different provisions of substantive law the legal effect of an electronic
18 record may be separate from the issue of whether the record contains a signature. For
19 example, where notice must be given as part of a contractual obligation, the effectiveness
20 of the notice will turn on whether the party provided the notice regardless of whether the
21 notice was signed. An electronic record attributed to a party under Section 109 would
22 suffice in that case, notwithstanding that it may not contain a signature.

23 2. Subsections (a) and (b) establish the fundamental premise of this Act: That the
24 form in which a record, signature or contract is generated, presented, communicated or
25 stored may not be the only reason to deny it legal recognition. On the other hand,
26 subsections (a) and (b) should not be interpreted as establishing the legal effectiveness of
27 any given record, signature or contract. For example, where a rule of law requires that the
28 record contain minimum substantive content, the legal effect will depend on whether the
29 record meets the substantive requirements. However, the fact that the information is set
30 forth in an electronic, as opposed to paper record, is irrelevant.

31 3. Subsections (c and d) are particularized applications of subsection (a). The purpose
32 is to validate and effectuate electronic records and signatures as the equivalent of writings,
33 subject to all of the rules applicable to the efficacy of a writing, except as such other rules
34 are modified by the more specific provisions of this Act.

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

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

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

5. Subsection (e) is a particularized application of Section 104, to make clear that parties retain control in determining the types of records to be used and accepted in any given transaction. For example, in the Chrysler recall hypothetical referred to in Note 2 to Section 104, although Chrysler cannot unilaterally require recall notices to be effective under this Act, it may indicate the method of recall in a purchase agreement with a customer. If the customer objects, the customer would have the right to establish reasonable requirements for such notices.

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

~~—— (1) A person, acting in person, by its agent or through its electronic device, manifests assent to a record or term if, acting with knowledge of, or after having an opportunity to review, the record or term it intentionally engages in conduct it knows or has reason to know will cause the other party to infer assent.~~

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

~~—— (3) If assent to a particular term is required by the substantive rules of law governing the transaction, a person, acting in person, by its agent or through its electronic~~

1 ~~device, does not manifest assent to the term unless there was an opportunity to review the~~
2 ~~term and the manifestation of assent relates specifically to the term:~~

3 ~~—— (4) A manifestation of assent may be proved in any manner, including showing~~
4 ~~that a procedure existed by which a person, acting in person, by its agent or through its~~
5 ~~electronic device must have engaged in conduct or operations that manifested assent to the~~
6 ~~record or term in order to proceed further in the transaction.]~~

7 **Reporter's Note to this Draft.** The Committee voted unanimously at the September,
8 1998 meeting to delete this section as unnecessary. Since the concept is not used
9 elsewhere in the statute, and since the provision was intended to merely track the
10 Restatement concepts of mutual assent, the Committee considered the provision
11 superfluous.

12
13 ~~**[SECTION 108. OPPORTUNITY TO REVIEW.** A person or electronic device~~
14 ~~has an opportunity to review a record or term only if it is made available in a manner that:~~
15 ~~—— (1) would call it to the attention of a reasonable person and permit review; or~~
16 ~~—— (2) in the case of an electronic device, would enable a reasonably configured~~
17 ~~electronic device to react to it.]~~

18 **Reporter's Note to this Draft:** See Note to deleted section 107 above.

19 ~~**SECTION 109. DETERMINATION OF REASONABLE SECURITY**~~
20 ~~**PROCEDURE.**~~

21 ~~—— [(a) The reasonableness of a security procedure is determined by the court as a~~
22 ~~matter of law.]~~

23 ~~—— (b) In determining the reasonableness of a security procedure, the following rules~~
24 ~~apply:~~

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

3 ~~_____ (2) A security procedure established by an organization for use in~~
4 ~~transactions among its members, or between other persons and the organization or its~~
5 ~~members is reasonable for the purposes for which it was established.~~

6 ~~_____ (3) Except as otherwise provided in paragraphs (1) and (2), reasonableness~~
7 ~~is determined in light of the purposes of the procedure and the circumstances at the time~~
8 ~~the parties agreed to or adopted the procedure, including the nature of the transaction,~~
9 ~~sophistication of the parties, volume of similar transactions engaged in by either or both of~~
10 ~~the parties, availability of alternatives offered to but rejected by a party, cost of alternative~~
11 ~~procedures, and procedures in general use for similar transactions.~~

12 ~~_____ (4) A reasonable security procedure may require the use of any security~~
13 ~~measures that are reasonable under the circumstances.~~

14 **Reporter's Notes to this Draft.** This section was deleted as no longer relevant in light of
15 the changes to section 107 below.

16 **SECTION 107 ~~110~~. EFFECT OF REQUIRING UNREASONABLE**
17 **SECURITY PROCEDURE.**

18 **ALTERNATIVE 1**

19 (a) [In a consumer transaction] If a person (the "requiring party") imposes; as a
20 condition of entering into a transaction with [a consumer] [another person], or otherwise is
21 responsible for a particular security procedure being used in a transaction ~~a requirement~~

1 ~~that the parties expressly agree to be bound by the results of a security procedure that is~~
2 ~~not reasonable~~, the following rules apply:

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

6 (B) application of the security procedure verified

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

9 _____(ii) the integrity of the informational content of the
10 electronic record,

11 the requiring party may not deny the source, or integrity of the informational content, of
12 the electronic record or electronic signature to which the security procedure was applied.

13 (2) If the requiring party relies on an electronic record or electronic
14 signature purporting to be that of the [consumer] [other party], the [consumer] [other
15 party] retains the right to deny the source of the electronic record or electronic signature,
16 or the integrity of the informational content of the electronic record.

17 ALTERNATIVE 2

18 (a) An agreement to be bound by the results of a security procedure is
19 unenforceable [in a consumer transaction].

20 END OF ALTERNATIVES

21 (b) The provisions of this section may not be varied by agreement.

1 ~~—— (b) A person does not impose a security procedure under subsection (a) if it makes~~
2 ~~reasonable alternative security procedures available to the other person, together with~~
3 ~~information which enables the other person to make an informed selection from among the~~
4 ~~offered procedures.~~

5 **Source:** New

6 **Reporter's Note to this Draft.** This section has been drafted in response to the
7 Committee's direction to prepare a provision which casts the risk of misattribution, and
8 informational error on the party that is responsible for a particular security procedure
9 being used in a transaction. One immediate difficulty in such a case is that the security
10 procedure being used may not have been injected into the transaction by either party, or it
11 may be virtually impossible to determine which party "required" the security procedure.
12 For example, the parties may be relying on a security procedure built into the software of
13 one or the other party, e.g., netscape's security procedure. In such a case it may be that
14 neither party is responsible for the security procedure because neither party consciously
15 selected the procedure. At the very least, the question of whether a party was responsible
16 for the use of the procedure may be difficult to determine.

17 Alternative 1 is a revision of the former section 110 stripped of the issue of the
18 reasonableness of the security procedure. Under this draft, regardless of the
19 reasonableness of a security procedure, the party not responsible for bringing the security
20 procedure into the transaction retains rights to deny attribution and content integrity of
21 records received by the requiring party, thereby putting the requiring party to its proof. At
22 the same time the provision binds the responsible party to records and signatures verified
23 by the security procedure and reasonably relied upon by the other party. These provisions
24 cannot be varied by agreement, and are no longer predicated on an agreement to be bound
25 by the results of the security procedure. If neither party was responsible for the use of the
26 security procedure this section would be inapplicable and the parties would be left to
27 prove the transaction in any reasonable manner.

28 Alternative 2 is more straightforward. It simply provides that an agreement to be
29 bound by the results of a security procedure regardless of the veracity of those results, is
30 not enforceable. Without such an agreement the parties will be left to prove the attribution
31 or content integrity of a record/signature by showing the efficacy of the security
32 procedure. An agreement to be bound to results obviates the necessity for the relying party
33 to convince the trier of fact that the security procedure is good and so establishes the
34 identity of the other party or content of the message. Instead all that need be shown is that
35 the security procedure was applied properly and that the result indicated the other party
36 was the sender and the content was as stated. The other party is then effectively denied the
37 ability to challenge the efficacy of the record/signature. If that agreement to be bound to
38 the results is denied effect, then the relying party must still prove the validity and quality
39 of the security procedure and the other party retains the ability to challenge the quality of
40 the procedure. If the parties do not expressly agree to be bound by the results of the

1 procedure, this alternative would not be applicable, and the proponent of the electronic
2 record or signature would be required to establish the validity of the record/signature.

3 **Illustration 1.** General Motors advises its franchisees that GM has established a
4 security procedure for ordering goods and that all parties must agree to be bound
5 by the results of the procedure. Through no fault of franchisee, bad guy sends an
6 electronic record which, upon application of the security procedure shows
7 franchisee as the buyer. Under Alternative 1, since GM was responsible for this
8 procedure being used, the franchisee would retain the right to deny that it is the
9 source of the order, and GM would be required to prove that the record was in fact
10 that of the franchisee under section 109. The agreement to be bound would be an
11 impermissible variation of the provisions of alternative 1.

12 If the underlying agreement as to the procedure were controlling, the franchisee
13 would bear the loss, since the electronic record would be attributable to the
14 franchisee. Under Alternative 2, that agreement is unenforceable (unless limited to
15 consumer transactions) and the franchisee retains the right to deny that it sent the
16 electronic record. GM would be put to its proof regarding the efficacy of the
17 security procedure or otherwise prove the order came from franchisee.

18 **Illustration 2.** Same facts as Illustration 1. If the bad guy is an employee of the
19 franchisee the result, in this case, would be no different. The franchisee remains
20 entitled to challenge the efficacy of the order placed by its employee, and GM
21 would have to establish attribution in fact under Section 109.

22 **Illustration 3.** GM advises its suppliers that GM has established a security
23 procedure for ordering goods and that all parties must agree to be bound by the
24 results of the procedure. Bad guy sends an order showing GM as the orderer of
25 \$50,000 of parts. Supplier relies on the order and ships the goods. Bad guy
26 intervenes and takes the goods. In Supplier's claim for payment, under Alternative
27 1, GM will be bound by the order so long as the security procedure was properly
28 applied and the supplier reasonably relied on it. Under Alternative 2, GM would
29 be allowed to deny that it sent the order because the agreement to be bound by the
30 results of the security procedure is unenforceable.

31 In a consumer context the general result will be that a vendor receiving an order will bear
32 the risk that the order did not come from the purported sender. If a security procedure is
33 proposed by the vendor, alternative 1 would make the vendor the requiring party. The
34 consumer would likely adopt the procedure in order to complete the transaction. If a
35 trustworthy procedure is used the vendor would be able to prove the efficacy of the
36 security procedure in order to establish consumer was the source of the order and should
37 be bound. If the security procedure was not trustworthy, the vendor would likely be
38 unable to establish consumer as the source of the record and would bear the loss. If the
39 consumer had agreed to be bound to the results of the procedure, alternative 2 would

1 preserve the consumer's ability to challenge the vendor's claims by making the agreement
2 unenforceable.

3 In transactions where neither party is responsible for the use of a particular security
4 procedure, as in the case of a consumer ordering from a web vendor under the netscape
5 security procedure residing on the consumer's computer, the parties are left to prove their
6 respective cases without aid of this section. Since the security procedure would be
7 adopted by the use of both parties without either party injecting it into the transaction,
8 Alternative 1 would not apply. Alternative 2 would be inapplicable since there would be
9 no agreement to be bound by the results.

10 In the event that a transaction is accomplished without any security procedure, this
11 Act, while validating the electronic records and signatures implemented in transactions
12 falling within the Scope of this Act, does not address whether such records and signatures
13 are otherwise legally binding or effective.

14 Among other commenters, the Bank Working Group has expressed its view that
15 the UETA should not include any rule which would provide a specific effect for a security
16 procedure. Rather, the use or non-use of security procedures would simply be one element
17 in a party's proof of records and signatures accomplished electronically. The Group's
18 letter to the Chair and Reporter has been distributed with this draft. WHETHER THE
19 UETA SHOULD LEAVE THE EFFECT OF SECURITY PROCEDURES TO OTHER
20 LAW IS A QUESTION THE COMMITTEE WILL NEED TO ADDRESS.

21 The draft provides an option to limit the alternative provisions to consumer
22 transactions. Given the function of these alternatives as protective, the draft provides that,
23 regardless of the alternative, this section may not be varied by agreement. THESE ARE
24 CRITICAL ISSUES FOR THE COMMITTEE'S CONSIDERATION.

25 **SECTION 108. PROVISION OF INFORMATION IN WRITING.**

26 (a) If a rule of law requires a person to provide information in writing to another
27 person, that requirement is satisfied if the information is provided in an electronic record
28 that is

29 (1) under the control of the person to which it is provided; and
30 (2) capable of retention for subsequent reference by the person to which it
31 is provided.

32 (b) The provisions of this section may not be varied by agreement in [a consumer
33 transaction].

1 **Source:** UETA Section 104(d) *Sept., 1998 Draft); Canadian Draft Uniform Electronic
2 Commerce Act

3 **Reporter's Note to this Draft.** This is a new section, previously a part of former Section
4 104 Exclusions from Scope. It is included in response to suggestions made in the Report
5 of the Task Force on State Law Exclusions to protect parties entitled to receipt of notice in
6 writing. The provision allows parties to provide information electronically so long as the
7 recipient has full control of the retention or disposition of the information once received.
8 The concern was prompted by the recognition that electronic information may be given to
9 a person while the person lacks the ability to copy or download the information.

10 **SECTION ~~202~~ 109. ATTRIBUTION OF ELECTRONIC RECORD TO PERSON.**

11 ~~_____ [ALTERNATIVE 1]~~

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

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

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

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

21 ~~_____ [ALTERNATIVE 2]~~

22 ~~_____ (a) An electronic record is attributable to a person if the electronic record resulted~~
23 ~~from the action of the person, acting in person, by its agent, or by its electronic agent~~
24 ~~device. Attribution may be proven in any manner, including by showing the efficacy of~~
25 ~~any security procedure applied to determine the person to ~~whom~~ which the electronic~~
26 ~~record was attributable.~~

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

Source: UETA Section 202 Alternative 2 (Sept. 1998 Draft); Originally derived from Article 2B.

Committee Vote: To adopt Alternative 2 - Yea - 3 Nay - 0 (October 1998)

Reporter's Notes: The language change in subsection (a) was made to conform to the language in Article 2B.

Alternative 1 was the provision as appeared in the Annual Meeting Draft. It was the result of the Committee's votes in April, 1998 to remove presumptions in this Section.

This draft retains the idea of attribution, including attribution to a person acting through an agent or electronic agent. It also indicates that the use of a security procedure will be an important aspect in establishing attribution. However, it does not set forth any rule of attribution under particular circumstances.

SECTION 203 110. DETECTION OF CHANGES AND ERRORS. If the parties act in conformity with a ~~reasonable~~ security procedure, ~~established by law, regulation, or agreement,~~ to detect changes or errors in the informational content of an electronic record, between the parties, the following rules apply:

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

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

Source: UETA Section 203 (Sept. 1998 Draft) - Originally derived from Article 2B.

Reporter's Note: No change from the September, 1998 Draft has been made except that the requirement that the security procedure be reasonable and the qualification that a security procedure must be established by law or agreement have each been deleted as unnecessary.

This section allocates the risk of errors and changes in transmission to the party that could have best detected the error or change through the proper application and use of a security procedure. If it is shown that application of the security procedure would have detected the error, the failure to apply the security procedure likely will result in the relying party bearing any resulting loss since the originating party will not be bound by the error. If it is shown that the security procedure would not have detected the error, subsection (1) will be inapplicable and the effect of any error will be determined under the applicable substantive law. If the security procedure requires the parties to communicate and one party fails to do so, that party will bear any loss under subsection (2). These results properly obtain regardless of the reasonableness of the procedure (since it must be effective to trigger the rule in (1)), or the manner in which the procedure was created.

THE COMMITTEE MAY WISH TO CONSIDER WHETHER SUBSECTION (2) ADDS ANYTHING TO THE SECTION. If the security procedure requires particular actions, subsection (1) requires both parties to comply. Subsection (2) is a specific application of subsection (1) since the actions contemplated under subsection (2) are the result of requirements under the security procedure. Subsection (1) could be redrafted as a single stand alone default rule.

~~**SECTION 204. INADVERTENT ERROR.**~~ [Moved to Section 116(a and d)]

~~**SECTION 302**~~ **111. EFFECT OF ELECTRONIC SIGNATURES.**

~~_____~~ **[ALTERNATIVE 1]**

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

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

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

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

~~_____~~ **[ALTERNATIVE 2]**

_____ (a) An electronic signature may be proven in any manner, including by showing that the electronic signature was signed in conformity with a security procedure for validating electronic signatures, or that a procedure existed by which the person, ~~acting in person, by its agent,~~ or by its electronic agent device, must have engaged in conduct or operations that signed the record or term in order to proceed further in the processing of the transaction.

[(b) A person bound by the operations of an electronic agent under Section 116 is deemed to have signed an electronic record produced by the agent on its behalf, whether or not the operations result in the attachment or application of an electronic signature to the electronic record].

~~(b)~~ (c) The effect of an electronic signature must ~~shall~~ be determined from the context and surrounding circumstances at the time of its execution or adoption.

Source: Subsections (a and c) from UETA Section 302 Alternative 2 (Sept. 1998 Draft); Subsection (b) from UETA Section 303 (Sept. 1998 Draft).

Committee Vote: To adopt Alternative 2 - Yea - 3 Nay - 0 (October 1998)

Reporter's Note to this Draft. The language change in subsection (a) was made to conform to the language in Article 2B.

1. Alternative 1 reflected the provision as it appeared in the Annual Meeting Draft. Alternative 2, adopted by the Committee in October, 1998, removes any statutory effect of an electronic signature verified by a security procedure. Instead, an electronic signature is proven in any reasonable manner, and it is likely that the efficacy of a security procedure will be critical in this proof. However, the effect of the signature is left to the context under subsection (c).

2. Subsection (b) has been moved to this section from former Section 303 because it relates to the existence of a signature. Its purpose is to establish that by programming an electronic agent, a party assumes responsibility for electronic records and operations "executed" by the program. While the electronic agent may or may not execute a symbol representing an electronic signature, the party programming the electronic agent has indicated its authentication of records and operations produced by the electronic agent within the parameters set by the programming. Accordingly, the party should be deemed

1 to have signed the records of the electronic agent. The effect of such a signature is left to
2 other law or agreement under subsection (c). **THE PROVISION HAS BEEN**
3 **BRACKETED FOR THE COMMITTEE'S CONSIDERATION REGARDING**
4 **WHETHER IT IS APPROPRIATE TO DEEM A RECORD SIGNED UNDER THE**
5 **CIRCUMSTANCES SET FORTH IN SUBSECTION (b).**

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

14 ~~**SECTION 303. OPERATIONS OF ELECTRONIC DEVICES.**~~ [Substance moved to
15 Section 116(b) and Section 111(b)](a) ~~A person that configures and enables an electronic~~
16 ~~device is bound by operations of the device.~~

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

21 **SECTION 304 112. NOTARIZATION AND ACKNOWLEDGMENT.**

22 If a rule of law requires that a signature be notarized or acknowledged, or provides
23 consequences in the absence of a notarization or acknowledgment, the requirement rule of
24 law is satisfied with respect to an electronic signature if a security procedure was applied
25 to the electronic signature which establishes ~~by clear and convincing evidence~~ the identity
26 of the person signing the electronic record [and that the electronic record has not been
27 altered since it was electronically signed].

28 **Source:** New

Reporter's Note: This provision has been added in response to the Task Force Report. The last clause has been bracketed because there is a question whether notarization and acknowledgment have the purpose of assuring content integrity. The clear and convincing standard has been deleted based on concerns raised at the October 1998 meeting that this standard is too stringent. The purpose of a notary is generally one of identification, and so long as a security procedure establishes identity by the normal preponderance of the evidence standard, that was considered to be sufficient.

~~SECTION 205. ORIGINALS: ACCURACY OF INFORMATION.~~ [COMBINED
WITH FORMER 206 IN NEXT SECTION]

~~—— (a) If a rule of law [or a commercial practice] requires a record to be presented or retained in its original form, or provides consequences if the record is not presented or retained in its original form, that rule of law requirement is satisfied met by an electronic record if [the electronic record is shown to reflect accurately] [there exists a reliable assurance as to the integrity of] the information set forth in the electronic record after it was first generated in its final form, as an electronic record or otherwise.~~

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

**~~SECTION 206~~ 113. RETENTION OF ELECTRONIC RECORDS;
ORIGINALS.**

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

1 the record, if the electronic record is shown to reflect accurately the information set forth
2 in the record after it was first generated in its final form as an electronic record or
3 otherwise.

4 (b) An electronic record reflects accurately the information in a record under
5 subsection (a), if:

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

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

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

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

18 ~~(cd)~~ A person satisfies subsection (a) by using the services of any other person; if
19 the conditions set forth in subsection (a) are met.

20 (e) If a rule of law [or a commercial practice] requires a record to be presented or
21 retained in its original form, or provides consequences if the record is not presented or

1 retained in its original form, that rule of law [or commercial practice] is satisfied by an
2 electronic record retained in accordance with subsection (a).

3 (df) A record retained as an electronic record in accordance with subsection (a)
4 satisfies rules of law requiring a person[, other than a governmental agency,] to retain
5 records for evidentiary, audit, or like purposes, until a governmental agency of this State
6 adopts rules of law specifically prohibiting the use of electronic records for specified
7 purposes within the jurisdiction of the governmental agency. However, this section does
8 not preclude a ~~federal or state~~ governmental agency of this State from specifying
9 additional requirements for the retention of records, either written or electronic, subject to
10 the agency's jurisdiction.

11 **Source:** UETA Sections 205 and 206 (Sept. 1998 Draft); Uncitral Model Articles 8 and
12 10; Illinois Model Sections 204 and 206.

13 **Reporter's Notes to This Draft:** Former sections 205 - Originals and 206 - Retention of
14 Records, overlapped in significant ways. This draft combines these provisions. The
15 general standard for retention in subsection (a) is derived from the former 205(a) standard
16 for an original. Subsection (b) provides a safe harbor for meeting the standard in
17 subsection (a), and is the provision for retention of electronic records from former section
18 206(a). Subsections (c and d) are from former section 206(b and c). Subsection (e) is
19 from former section 205(a) and makes records retained in accordance with the standard in
20 subsection (a) valid as originals. Finally, subsection (f) is an expansion of former section
21 206(d) which is necessary to assure that governmental agencies are required to accept
22 records retained electronically for evidentiary, audit and similar record retention functions,
23 unless the agency specifically requires another medium.

24 **Reporter's Note:** This section deals with the serviceability of electronic records as
25 retained records and originals. As was noted at the May, 1997 meeting, the concept of an
26 original electronic document is problematic. For example, as I draft this Act the question
27 may be asked what is the "original" draft. My answer would be that the "original" is either
28 on a disc or my hard drive to which the document has been initially saved. Since I
29 periodically save the draft as I am working, the fact is that at times I save first to disc then
30 to hard drive, and at others vice versa. In such a case the "original" may change from the
31 information on my disc to the information on my hard drive. Indeed, as I understand
32 computer operations, it may be argued that the "original" exists solely in RAM and, in a
33 sense, the original is destroyed when a "copy" is saved to a disc or to the hard drive. In any

1 event, the concern focuses on the integrity of the information, and not with its
2 "originality."

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

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

21 Since requirements for "originals" are often the result of commercial practice and not an
22 actual rule of law, the section includes the bracketed language regarding requirements
23 derived from commercial practice. As a policy matter it is not at all clear that legislation
24 should override established commercial practice. **THIS PROVISION (now in**
25 **subsection (e)) REMAINS BRACKETED AS A QUESTION WHICH MUST BE**
26 **RESOLVED BY THE DRAFTING COMMITTEE.**

27 So long as there exists reliable assurance that the electronic record accurately
28 reproduces the information, this section continues the theme of establishing the functional
29 equivalence of electronic and paper-based records. This is consistent with Fed.R.Evid.
30 1001(3) and Unif.R.Evid. 1001(3) (1974) which provide:

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

33 This draft adopts as the appropriate standard that noted in the rules of evidence.

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

37 At the May, 1997 meeting concern was expressed that retained records may become
38 unavailable because the storage technology becomes obsolete and incapable of
39 reproducing the information on the electronic record. Subsection (b)(1) addresses this
40 concern by requiring that the information in the electronic record "remain" accessible, and

subsection (b)(2) addresses the need to assure the integrity of the information when the format is updated or changed.

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

SECTION ~~404~~ 114. ADMISSIBILITY INTO EVIDENCE.

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

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

or

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

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

Source: UETA Section 404 (Sept. 1998 Draft); Uncitral Model Article 9; Illinois Model Section 205.

Reporter's Note: Like section 106, subsection (a)(1) prevents the nonrecognition of electronic records and signatures solely on the ground of the media in which information is presented. Subsection (a)(2) also precludes inadmissibility on the ground an electronic record is not an original.

Nothing in this section relieves a party from establishing the necessary foundation for the admission of an electronic record.

Subsection (b) gives guidance to the trier of fact in according weight to otherwise admissible electronic evidence. **IT HAS BEEN BRACKETED FOR THE DRAFTING COMMITTEE'S CONSIDERATION** in light of the questionable propriety of statutorily directing a court in the manner of consideration of evidence.

1 **SECTION 401 115. FORMATION OF CONTRACT AND VALIDITY.**

2 (a ~~b~~) If an electronic record initiated by a person, or by its party or an electronic
3 agent device, evokes an electronic record in response a contract is formed in the same
4 manner and with the same effect as if the electronic records were not electronic. A contract
5 is formed, if at all:

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

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

11 (b 3) The terms of a contract are determined by the substantive rules of law
12 applicable to the particular contract.

13 (a) ~~In an automated transaction, the following rules apply: [COMPARE SECTION~~
14 ~~116(c) INFRA]~~

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

21 ~~————— (2) A contract may be formed by the interaction of an person's electronic~~
22 ~~device and an individual. A contract is formed by the interaction if the individual~~

1 ~~performs actions that the individual knows or reasonably should know will cause the~~
2 ~~device to complete the transaction or performance, or which are clearly indicated to be an~~
3 ~~acceptance, regardless of other expressions or actions by the individual to which the~~
4 ~~individual cannot reasonably expect the electronic device to react.~~

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

7 ~~(A) terms of the parties' agreement;~~

8 ~~_____ (B) terms that an the electronic device could takes into account;~~
9 ~~and~~

10 ~~_____ (C) to the extent not covered by subparagraph (1A) or (2B), terms~~
11 ~~provided by law.~~

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

14 **Source:** UETA Section 401(b) and (a)(3) (Sept. 1998 Draft); Article 2B Draft Section
15 2B-204; Uncitral Model Article 11.

16 **Reporter's Note:** The language in subsection (a) has been revised to conform with the
17 parallel provisions in Article 2B.

18 This section has been significantly revised. The provisions in former section 401
19 relating to automated transactions have been moved to the next section. The subsection
20 addressing the efficacy of electronic contracts has been moved to section 106 regarding
21 general efficacy of electronic records, signatures and contracts.

22 The balance of the section now simply provides that contract formation and
23 determination of resulting terms are a function of the law underlying the transaction. The
24 only change wrought by this section is to provide that the timing of the contract is based
25 on receipt and not sending, reversing the mailbox rule.

26 **SECTION 116. OPERATIONS OF ELECTRONIC AGENTS;**

27 **AUTOMATED TRANSACTIONS.** (a) In this section, "inadvertent error" means an
28 error by an individual made in dealing with an electronic agent of another person if the

1 electronic agent of the other person did not allow for the prevention or correction of the
2 error.

3 (b) Operations of an electronic agent are the acts of a person if the person used the
4 electronic agent for such purposes.

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

6 (1) A contract may be formed by the interaction of electronic agents of the
7 parties, even if no individual was aware of or reviewed the electronic agent's actions or the
8 resulting terms and agreements.

9 (2) A contract may be formed by the interaction of a person's electronic
10 agent and an individual. A contract is formed by the interaction if the individual performs
11 actions that it is free to refuse to perform which the individual knows or has reason to
12 know will cause the electronic agent to complete the transaction or performance.

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

17 (1) promptly notifies the other person of the error and that the individual
18 did not intend the electronic record received by the other person;

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

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

Source: UETA Sections 204, 303(a) and 401(a)(Sept. 1998 Draft) - Originally derived from Article 2B Draft.

Reporter's Notes to This Draft: This section brings together all provisions from the September, 1998 Draft which deal with the use of Electronic agents. It provides for the effectiveness of actions taken through the operations of electronic agents, clarifies that contracts can be entered

1 into by machines, and addresses the idea of inadvertent error when an individual is dealing
2 with a machine.

3 Former Section 303(a) has been revised to make the operations of electronic agents
4 the acts of the person using the agent for the purposes accomplished. This makes the
5 section parallel to the provision in Article 2B, and addresses concerns of the ABA
6 Electronic Agents Task Force regarding the strict liability aspect of the former provision.
7 By equating the operations with acts of a person, the legal effect of a person's acts,
8 accomplished through the operations of an electronic agent, are left to the substantive law
9 governing the transaction.

10 Former section 204 has been included without substantive change. The second
11 sentence of former section 401(a)(1) has been deleted based on comments at the last
12 meeting that it was unnecessary. Based on the same concerns, minor changes for
13 clarification to former section 401(a)(2) have been made.

14 **Reporter's Notes:**

15 **1. Operations of Electronic agents.** Formerly Section 303(b).

16 Section 116(b) makes clear that the party that sets operations of an electronic agent
17 in motion is responsible for the records and signatures resulting from such operations. A
18 party is bound by the actions of a computer program designed to act without human
19 intervention, as well as electronic and automated means such as telecopy and facsimile
20 machines used by a party.

21 A Task Force of the ABA Committee on the Law of Cyberspace considered the
22 issue of electronic agents at the mid-winter working meeting in Atlanta, January 15-16,
23 1998. A proposed alternative based on that meeting has been included in the Reporter's
24 Memorandum for this draft.

25 **2. Automated Transactions.** Formerly section 401(a).

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

31 B. Subsection (c)(2) addresses the circumstance of an individual dealing with an
32 electronic agent.

33 As noted in a number of comments at the January, 1998 meeting, whether one
34 knows that one is dealing with an electronic agent should be irrelevant, so long as the
35 individual proceeds with actions it knows or reasonably should know will result in
36 accomplishment of the ends desired. Concerns previously expressed by observers that
37 individuals may not know what contemporaneous statements made by the individual
38 would be given effect because of the possibility of contemporaneous or subsequent human
39 review, have been addressed by limiting those actions of the individual which may result
40 in a contract to those which the individual would reasonably expect to result in a contract.
41 This will provide the party employing an electronic agent with an incentive to make clear
42 the parameters of the agent's ability to respond. If the party employing the electronic
43 agent provides such information, the individual's act of proceeding on the basis of
44 contemporaneous actions or expressions not within the parameters of the agent would be

1 unreasonable and such actions and expressions could not be the basis for contract
2 formation.

3 **3. Inadvertent Error.** Formerly section 204.

4 This section attempts to address the issue of human error in the context of an
5 automated transaction. The reason for attempting to address this issue is that inadvertent
6 errors, such as a single keystroke error, do occur, and are difficult, if not impossible to
7 retrieve, given the speed of electronic communications. However, the definition of
8 "inadvertent error" would allow a vendor to provide an opportunity for the individual to
9 confirm the information to be sent, in order to avoid the operation of this provision. By
10 providing an opportunity to an individual to review and confirm the information initially
11 sent, the other party can eliminate the possibility of the individual defending on the
12 grounds of inadvertent error since the electronic agent, through confirmation, allowed for
13 correction of the error.

14 **SECTION ~~402~~ 117. TIME AND PLACE OF SENDING AND RECEIPT.**

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

19 (b) Unless otherwise agreed between the sender and the recipient, an electronic
20 record is received when the electronic record enters an information processing system in a
21 form capable of being processed by that system that the recipient uses or has designated
22 for the purpose of receiving electronic records or information and from which the recipient
23 is able to retrieve the electronic record. ~~s in a form capable of being processed by that~~
24 ~~system, if the recipient uses or has designated that system for the purpose of receiving~~
25 ~~such an electronic record or information.~~ An electronic record is also received when the
26 recipient learns of its content from a record.

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

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

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

11 (2) If the sender or the recipient does not have a place of business, the place
12 of business is the sender's or recipient's residence, as the case may be.

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

15 [(f) Receipt of an electronic acknowledgment establishes that a record was
16 received but, in itself, does not establish that the content sent corresponds to the content
17 received.]

18 **Source:** UETA Sections 402 and 403(b) (Sept. 1998 Draft); Uncitral Model Article 15.
19 **Reporter's Note to this Draft.** This section has been revised for clarity and to
20 incorporate former subsection 403(b) in light of the deletion of the balance of former
21 section 403.

22 **Reporter's Note:**

23 1. This section provides default rules regarding when an electronic record is sent and
24 when and where an electronic record is received. This section does not address the
25 efficacy of the record that is received. That is, whether a record is unintelligible or
26 unusable by a recipient is a separate issue from whether that record was received.

2. Subsection (a) now requires that information be properly addressed or otherwise directed to the recipient before it will be considered sent.

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

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

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

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

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

6. Subsection (f), from former section 403, provides that receipt of an acknowledgment does not establish the content of the message, but simply that it was received. It is a holdover from former Section 403 and HAS BEEN BRACKETED FOR THE COMMITTEE'S CONSIDERATION WHETHER IT IS NECESSARY.

~~SECTION 403. ELECTRONIC ACKNOWLEDGMENT OF RECEIPT.~~

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

~~———— (1) If the sender indicates in the record or otherwise that the record is conditional on receipt of an electronic acknowledgment, the record does not bind the~~

1 ~~sender until acknowledgment is received, and the record is no longer effective if~~
2 ~~acknowledgment is not received within a reasonable time after the record was sent.~~

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

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

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

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

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

15 **Source:** Uncitral Model Article 14; Article 2B.

16 **Reporter's Note:** This section was deleted by vote of the Committee Yea- 3 Nay - 0 at the
17 October 1998 meeting. Subsection (b) was moved to section 117(f).

18 **SECTION 405 118. CONTROL OF TRANSFERABLE RECORDS.** ~~If the~~
19 ~~identity of the person entitled to enforce a transferable record can be reliably determined~~
20 ~~from the record itself or from a method employed for recording, registering, or otherwise~~
21 ~~evidencing the transfer of interests in such records, the person entitled to enforce the~~
22 ~~record is deemed to be in possession of the record.~~

1 (a) A person having control of a transferable record is deemed to be [in possession]
2 [the holder] of the transferable record.

3 (b) A person has control of a transferable record if ~~the record itself~~ or a method
4 employed for recording, registering, or otherwise evidencing the transfer of interests in
5 such records reliably establishes that person as the person with the right to enforce the
6 transferable record.

7 (c) A person has control of a transferable record under subsection (b) if the record
8 or records comprising the transferable record are created, stored, and assigned in such a
9 manner that:

10 (1) a single authoritative copy of the record or records exists which is
11 unique, identifiable, and except as otherwise provided in paragraphs (4), (5), and (6),
12 unalterable;

13 (2) the authoritative copy identifies the person asserting control as the
14 assignee of the record or records;

15 (3) the authoritative copy is communicated to and maintained by the person
16 asserting control or its designated custodian;

17 (4) copies or revisions that add or change an identified assignee of the
18 authoritative copy can be made only with the consent of the person asserting control;

19 (5) each copy of the authoritative copy and any copy of a copy is readily
20 identifiable as a copy that is not the authoritative copy; and

21 (6) any revision of the authoritative copy is readily identifiable as an
22 authorized or unauthorized revision.

Source: Subsection (b) derived from Oklahoma Model Section III.B.2;subsection (c) Revised Article 9, Section 9-105..

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

The focus of this section has been clarified and sharpened. Like Revised Article 9 section 9-105 (from which subsection (c) is taken), this provision is intended to provide an analog to possession of a tangible instrument. "Control" is intended to serve as the functional equivalent of possession of a written token. If control of the transferable record can be established, then it is possible to invoke the rules of Article 3 (if the transferable record is the unwritten equivalent of a note) to establish one's rights as a holder in due course. The question of the necessity to also provide imputation of indorsements is continuing to be discussed, and may be necessary. The question of indorsements can be mooted by adopting the provision making the person in control the "holder", since then all indorsements will necessarily be imputed.

At the ABA Committee on the Law of Cyberspace working meeting in Atlanta January 15-16, discussions about the proper formulation for including electronic tokens in the UETA were had with members of the CLC committee including representatives from the Federal Reserve. The memorandum from Professors Jane Winn and Paul Shupack to the Chair and Reporter will be available for the Committee's consideration in Richmond.

PART 3

~~ELECTRONIC SIGNATURES~~

PART 4

~~ELECTRONIC CONTRACTS AND COMMUNICATIONS~~

PART 5 2

GOVERNMENTAL ELECTRONIC RECORDS

SECTION 5 201. CREATION AND RETENTION OF ELECTRONIC RECORDS AND CONVERSION OF WRITTEN RECORDS BY GOVERNMENTAL AGENCIES.

~~[Unless expressly prohibited by statute, each]~~ [Each] governmental agency of this State shall determine if, and the extent to which, it will create and retain electronic records ~~instead of written records~~ and convert written records to electronic records. ~~[The~~

1 ~~[designated state officer]~~ shall adopt rules governing the disposition of written records
2 after conversion to electronic records.]

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

5 **Reporter's Note:** See Notes following Section 203.

6 **SECTION 5 202. RECEIPT ACCEPTANCE AND DISTRIBUTION OF**
7 **ELECTRONIC RECORDS BY GOVERNMENTAL AGENCIES.**

8 (a) Except as otherwise provided in Section 113(f), ~~[Except as expressly prohibited~~
9 ~~by statute each]~~ ~~[each]~~ governmental agency of this State shall determine whether, and the
10 extent to which, it will send and ~~receive~~ accept electronic records and electronic signatures
11 to and from other persons, and otherwise create, use, store, and rely upon electronic
12 records and electronic signatures.

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

15 (1) the manner and format in which the electronic records must be created,
16 sent,
17 received, and stored[, and the systems established for such purposes];

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

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

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

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

~~(d c)~~ Except as otherwise provided in Section 113(f), this [Act] does not require any governmental agency of this State to use or permit the use of electronic records or electronic signatures.

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

Reporter's Note: See Notes following Section 203.

~~—— SECTION 5 203. [DESIGNATED STATE OFFICER] TO ADOPT STATE STANDARDS. The [designated state officer] may adopt regulations setting forth rules, standards, procedures, and policies for the use of electronic records and electronic signatures by governmental agencies. If appropriate, those regulations must specify differing levels of standards from which implementing governmental agencies may choose in implementing the most appropriate standard for a particular application.~~

~~SECTION 504 203. INTEROPERABILITY. To the extent practicable under the circumstances, regulations adopted by [designated state officer] or a governmental agency relating to the use of electronic records or electronic signatures must be drafted in a~~

1 ~~manner~~ Regulations adopted by a governmental agency of this State pursuant to Section
2 202 must be designed to encourage and promote consistency and interoperability with
3 similar requirements adopted by other governmental agencies of this and other States and
4 the federal government, and non-governmental persons interacting with governmental
5 agencies of this State. If appropriate, those regulations must specify differing levels of
6 standards from which ~~implementing~~ governmental agencies of this State may choose in
7 implementing the most appropriate standard for a particular application.

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

9 **Reporter's Notes to Part 2.** This Part addresses the expanded scope of this Act.

10 **Committee Votes:** To delete bracketed provisions in sections 201, 202 and to delete
11 former section 503. Yea - 3 Nay - 0 (October, 1998)

12 1. Section 201 is derived from former subsection 501(a) and authorizes state agencies to
13 use electronic records and electronic signatures generally for intra-governmental purposes,
14 and to convert written records and manual signatures to electronic records and electronic
15 signatures. By its terms it leaves the decision to use electronic records or convert written
16 records and signatures to the governmental agency. It also authorizes the destruction of
17 written records after conversion to electronic form. The bracketed language requiring the
18 appropriate state officer to issue regulations governing such conversions was deleted by
19 the Committee at the October, 1998 meeting. The Committee also deleted former section
20 503 because it was considered inappropriate to provide for a single mechanism for
21 promulgation of regulations in every state.

22 2. Section 202 has been revised along the model of the pending Illinois legislation and
23 broadly authorizes state agencies to send and receive electronic records and signatures in
24 dealing with non-governmental persons. Again, the provision is permissive and not
25 obligatory (see subsection (d)). However, it has been clarified to provide that with respect
26 to electronic records used for evidentiary purposes, Section 113 will apply unless a
27 particular agency expressly opts out.

28 3. Section 203 requires regulating authorities to take account of consistency in
29 applications and interoperability to the extent practicable when promulgating regulation.
30 This section is critical in addressing the concerns of many at our meetings that inconsistent
31 applications may promote barriers greater than currently exist.

32 **PART 6 3**

33 **MISCELLANEOUS PROVISIONS**

1 **SECTION 6 301. SEVERABILITY CLAUSE.** If any provision of this [Act] or
2 its application to any person or circumstance is held invalid, the invalidity does not affect
3 other provisions or applications of this [Act], which can be given effect without the invalid
4 provision or application, and to this end the provisions of this [Act] are severable.

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

6 **SECTION 6 302. EFFECTIVE DATE.** This [Act] takes effect....

7 **Source:**

8 **SECTION 6 303. SAVINGS AND TRANSITIONAL PROVISIONS.**

9 **Source:**