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

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

EX OFFICIO

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

AMERICAN BAR ASSOCIATION ADVISORS

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

EXECUTIVE DIRECTOR

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

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

TABLE OF CONTENTS

PART 1

GENERAL PROVISIONS

SECTION 101. SHORT TITLE.
SECTION 102. DEFINITIONS.
SECTION 103. SCOPE.
SECTION 104. TRANSACTIONS SUBJECT TO OTHER LAW.
SECTION 105. VARIATION BY AGREEMENT.
SECTION 106. APPLICATION AND CONSTRUCTION.
SECTION 107. COURSE OF PERFORMANCE, COURSE OF DEALING, AND USAGE
OF TRADE.
[SECTION 1078. MANIFESTING ASSENT.]
[SECTION 1089. OPPORTUNITY TO REVIEW.]
SECTION 10910. DETERMINATION OF COMMERCIALLY REASONABLE SECURITY
PROCEDURE; COMMERCIALLY UNREASONABLE SECURITY
PROCEDURE; NO SECURITY PROCEDURE.
SECTION 110. EFFECT OF REQUIRING A COMMERCIALLY UNREASONABLE
SECURITY PROCEDURE.
SECTION 111. OBLIGATION OF GOOD FAITH.
SECTION 112. GENERAL PRINCIPLES OF LAW APPLICABLE.

PART 2

ELECTRONIC RECORDS GENERALLY

SECTION 201. LEGAL RECOGNITION OF ELECTRONIC RECORDS.
SECTION 202. ATTRIBUTION OF ELECTRONIC RECORD TO A PERSON PARTY.
SECTION 203. DETECTION OF CHANGES AND ERRORS.
SECTION 204. ORIGINALS - INFORMATION ACCURACY.
SECTION 205. RETENTION OF ELECTRONIC RECORDS.

PART 3

ELECTRONIC SIGNATURES GENERALLY

SECTION 301. LEGAL RECOGNITION OF ELECTRONIC SIGNATURES.
SECTION 302. ELECTRONIC SIGNATURES EFFECT AND PROOF.
SECTION 303. [SIGNATURES BY] [OPERATIONS OF] ELECTRONIC AGENTS.
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
GOVERNMENTAL ELECTRONIC RECORDS

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

PART 6
MISCELLANEOUS PROVISIONS

SECTION 601. SEVERABILITY.
SECTION 602. EFFECTIVE DATE.
SECTION 603. SAVINGS AND TRANSITIONAL PROVISIONS.
PART 1

GENERAL PROVISIONS

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

SECTION 102. DEFINITIONS.

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

(1) "Agreement" means the bargain of the parties in fact as found in their language or inferred from other circumstances, including course of performance, course of dealing and usage of trade as provided in this Act. Whether an agreement has legal consequences is determined by this Act, if applicable, or otherwise by other applicable rules of law.

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

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

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

Notes to This Draft: At the September, 1997 Meeting the definition of agreement which included terms to which a party manifested assent was rejected. The consensus of both the Committee and observers was that there was no need to separate manifestations of assent from the language and circumstances which comprise the bargain in fact of the parties as part of the definition of agreement. Rather the Reporter was directed to return to the definition of agreement in the Uniform Commercial Code. Accordingly, the definition in the November Draft was taken from the most recent revision to Article 1.

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

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

**Reporter's Note:** Whether the parties have reached an agreement is determined by their express language and surrounding circumstances. The Restatement of Contracts §3 provides that "An agreement is a manifestation of mutual assent on the part of two or more persons. A bargain is an agreement to exchange promises or to exchange a promise for a performance or to exchange performances."
The Uniform Commercial Code specifically includes in the circumstances from which an agreement may be inferred "course of performance, course of dealing and usage of trade..." as defined in the UCC.

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

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

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

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

**Textual References:** Section 204. Inadvertent Error; Section 401. Formation and Validity.
Committee Vote: To delete references to governmental and commercial: Committee 4 Yes (Chair broke tie) - 3 No; Observers 19 Yes - 1 No. (Jan. 1998)

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

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

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

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

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

Reporters Note: This definition was deleted as too broad, and unnecessary in light of the approach to Scope and exclusions adopted by the Committee at the January, 1998 meeting. See Reporter's Notes to Sections 103 and 104 below.
"Computer program" means a set of statements or instructions to be used directly or indirectly to operate in an information processing system in order to bring about a certain result. The term does not include informational content created or communicated as a result of the operation of the system.

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


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

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

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

Source: UCC Section 1-201(11)

Textual References: Section 401. Formation and Validity.

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

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


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

Reporter's Note: This definition serves to assure that the Act will be applied broadly as new technologies develop. While not all technologies listed are technically "electronic" in nature (e.g., optical fiber technology), the need for a recognized, single term warrants the use of "electronic" as the defined term. Query whether the definition is broad enough?
"Electronic agent" means a computer program or other electronic or automated means used, selected, or programmed by a person to initiate or respond to electronic records or performances in whole or in part without review by an individual.

Source: Article 2B Draft Section 2B-102(a)(18).
Reporter's Note: An electronic agent, as a computer program or other automated device employed by a person, is a tool of that person. As a general rule, the employer of a tool is responsible for the results obtained in the use of that tool since the tool has no independent volition of its own. However, an electronic agent by definition is capable, within the parameters of its programming, of initiating, responding or interacting with other parties or their electronic agents once it has been activated by a party, without further attention of that party. This draft contains provisions dealing with the efficacy of, and responsibility for, actions taken and accomplished by electronic agents in the absence of human intervention.

While this Act proceeds on the paradigm that an electronic agent is capable of performing only within the technical strictures of its preset programming, it is conceivable that, within the useful life of this Act, electronic agents may be created with the ability to act autonomously, and not just automatically. That is, through developments in artificial intelligence, a computer may be able to "learn through experience, modify the instructions in their own programs, and even devise new instructions." Allen and Widdison, "Can Computers Make Contracts?" 9 Harv. J.L.&Tech 25 (Winter, 1996). At such time as this may occur, "Courts may ultimately conclude that an electronic agent is equivalent in all respects to a human agent..." Article 2B-102, Reporter's Note 10.

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

"Electronic record" means a record created, stored, generated, received, or communicated by electronic
means., such as information systems, computer equipment and
programs, electronic data interchange, electronic mail, or voice
mail, facsimile, telex, telecopying, scanning, and similar
technologies.

Source: Article 2B Draft Section 2B-102(a)(19)
Textual References: Passim.
Notes to this Draft: The last clause has been deleted and moved
to the comment to avoid confusion. Comments to the prior draft
suggested that these means of accomplishing an electronic record,
were themselves electronic records. The list of mechanisms has
been included in the comment/note below.
Reporter's Note: An electronic record is a subset of the broader
defined term "record." Unlike the term "electronic message" used
in Article 2B, the definition is not limited to records intended
for communication, but extends to any information contained or
transferred in an electronic medium. It is also used in this Act
as a limiting definition in those provisions in which it is used.
Electronic means for creating, storing, generating,
receiving or communicating electronic records include information
processing systems, computer equipment and programs, electronic
data interchange, electronic mail, or voice mail, facsimile,
telex, telecopying, scanning, and similar technologies.

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

Source: UCC Section 1-201(39); Illinois Model Section 200(3).
Textual References: Passim.
Notes to This Draft: The last clause has been deleted as
redundant of the definition of signature.
Reporter's Note: As with electronic record, this definition is a
subset of the broader defined term "signature." The purpose of
the separate definition is principally one of clarity in
extending the definition of signature to the electronic
environment.

This definition has been simplified by using the defined
term "signature" within this definition. The defined term
"signature" has been expanded from the standard UCC definition to
incorporate specifically the attributes normally attached to a
written signature, and to track the concept of authentication as
declared in Article 2B. The new definition of "signature"
reflects the Committee's direction to delete the term
"authenticate" from the August Draft and incorporate that
definition into "signature."

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

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

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

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

Source: Revised Article 1 Section 1-201(22) (Sept. 1997 draft)
Committee Vote: To delete Section 111 Obligation of Good Faith -
Committee 6 Yes - 1 No; Observers 7 Yes - 5 No. (Jan. 1998)
Notes to This Draft: The definition and obligation of good faith
(former Section 111) have been deleted. The Committee's view was
that the obligation of good faith was an issue to be determined
as a matter of the substantive law applicable to the underlying
transaction. Accordingly, the issue of whether good faith is
required, and its impact on a given transaction is left to the
substantive law applicable to the particular transaction outside
this Act.
"State Governmental agency" means any executive[, legislative, or judicial] agency, department, board, commission, authority, institution, or instrumentality of this State or of any county, municipality or other political subdivision of this State.

Source: New.


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

Reporter's Note: Although the approach to the Scope of this Act has been revised (See Notes to Section 103), this definition is important in the context of Part 5. The reference to legislative and judicial agencies, etc. has been bracketed in light of comment from members of the Committee that these should not be included. The Reporter seeks direction from the Committee on whether the legislative and judicial branches should be excluded.

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

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

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

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

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

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

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

Source: Article 2B Draft Section 2B-102(25).
Reporter's Note: This definition has been added to differentiate information in an electronic record, which includes all data forming part of an electronic record, with the informational content of an electronic record which is the portion of the electronic record intended actually to be used by a human being. The example from Article 2B most clearly establishing this distinction is the Westlaw user who uses the search program to retrieve a case. The search program would be information, but only the case retrieved would be informational content.

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

Source: UNCITRAL Model Article 2(f); Article 2B Draft Section 2B-102(a)(24).
Textual References: Section 402. Time and Place of Sending and Receipt.
Reporter's Note: This term is used in Section 402 regarding the time and place of receipt of an electronic record. It is somewhat broader than the Article 2B definition. Query the accuracy and completeness of this definition?

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

Source: Illinois Model Section 103(22) (June 4 Interim Draft).
Reporter's Note: As with the provisions on receipt in Section 402, a notice sent to a party must be in a proper format to permit the recipient to use and understand the information. For
example, sending a message to a recipient in the United States in
Chinese would not suffice to notify the recipient of the content
of the message, in the absence of proof that the recipient
understood Chinese. Similarly, sending a notice in WordPerfect
7.0 may not be appropriate when many people do not have the
capability to convert from that format. In such a case, a more
universal format such as ASCII would be required.

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

Source: UCC Section 1-201(28).
Textual References: None.
Reporter's Note: Although, this is a standard Conference
definition, it has been deleted since it is not used.

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

Source: CC Section 1-201(30).
Textual References: Passim
Reporter's Note: This is the standard Conference formulation for
this definition.

[ALTERNATIVE 1]

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

Source: UCC Section 1-201(31)

[ALTERNATIVE 2]

(1517) "Presumption" means that when a fact or group
of facts giving rise to a presumption (the "basic fact") exists,
the existence of the fact to be assumed upon a finding of the
basic fact (the "presumed fact") must be assumed unless and until
the party against whom the presumption is directed produces
evidence which would support a finding of the non-existence of
the presumed fact. "Presumed" has a corresponding meaning.

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

[ALTERNATIVE 3]

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

Source: Derived from revision suggested by Committee on Style.

Textual References: Section 110. Effect of Requiring Commercially
Unreasonable Security Procedure. Section 202. Attribution of
Electronic Record. Section 203. Detection of Changes and
Section 403. Electronic Acknowledgement of Receipt.

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

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

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

In all civil actions and proceedings not otherwise provided
for by statute, by judicial decision, or by these rules, a
presumption imposes on the party against whom it is directed
the burden of proving that the nonexistence of the presumed fact is more probable than its existence.

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

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

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

The effect of this definition also would result in the shifting of the burden of persuasion. In addition, while a presumption may be viewed as a legally required inference, it is not considered to be a substitute for evidence of the presumed fact.


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

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

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

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

2 McCormick on Evidence §344. Similarly, when a party proves the implementation of a commercially reasonable security procedure, the other party may destroy the presumption (e.g., attribution, lack of errors, etc.), by directly denying the presumed fact (attribution, error, etc). However, a jury question may remain based on the strength of the evidence of the security procedure.
and the natural inference that, if followed the security
procedure would demonstrate that the electronic record was that
of the sender, did not contain errors, etc.

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

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

Source: Article 2B Draft Section 2B-102(a)(37).
Textual References: Section 102. "Automated Transaction,
"Electronic Record," "Signature," "Transferable Record,
"Writing". Section 105. Variation by Agreement. Section 107.
Manifestation of Assent. Section 108. Opportunity to Review.
Section 201. Legal Recognition of Electronic Records. Section
203. Detection of Changes and Errors. Section 205.
Originals: Accuracy of Information. Section 206. Retention of
Electronic Records. Section 302. Electronic Signatures: Effect
and Proof. Section 401. Formation and Validity. Section 403.
Electronic Acknowledgement of Receipt. Section 405. Transferable
Records. Section 501. Creation and Retention of Records...
Reporter's Note: This is the standard Conference formulation for
this definition.

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

Source: Oklahoma Model Section II.F; Illinois Model Section
200(7).
Textual References: Section 201. Legal Recognition of Electronic
Records. Section 205. Originals: Accuracy of Information.
Section 206. Retention of Electronic Records. Section 301. Legal
Recognition of Electronic Signatures.
Reporter's Note: The definition is drafted broadly. The former limitation relating to commercial and governmental transactions, has been deleted in light of the Committee's vote regarding the manner of defining the Scope of this Act.

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

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


Notes to This Draft: Edited for clarity and to more closely track Article 2B definition of "attribution procedure," and also to eliminate the requirement that, as defined, a security procedure must be commercially reasonable. The element of commercial reasonableness remains important in the determination of the applicability of presumptions which may attach to the use of security procedures in Sections 202, 203 and 302.
Reporters Note: Limiting security procedures to those which are either agreed to or adopted by parties or established by law or regulation, together with the requirement that only commercially reasonable security procedures give rise to limited presumptions, eliminates much of the concern over the creation of the limited presumptions in Sections 202, 203 and 302. The effect of commercially unreasonable security procedures imposed by one party is addressed in Section 110. In such cases the party at risk is the party imposing the commercially unreasonable procedure. In this way, the party with the greatest incentive to assess the risk of proceeding in a transaction with commercially unreasonable procedures will bear the loss.

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

(19) "Sign" means the execution or adoption of a signature by a person or the person’s electronic agent.

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


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

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

†A identify the party that person;

†B adopt or accept a term or a record; or

†C establish the informational integrity of a record or term that contains the signature or to which a record containing the signature refers.
"Sign" means the execution or adoption of a signature by a person or the person's electronic agent.

Source: UCC Section 1-201(39); Article 2B Draft Section 2B-102(a)(3)
Notes to This Draft: Edited for clarity.
Reporter's Note: At the September Drafting Meeting, the consensus of the Committee and observers was to go back to the definition of signature, and to delete the definition of "authenticate." Given the purpose of this Act to equate electronic signatures with written signatures, the sense was that retaining signature as the operative word would better accomplish that purpose. However, the idea of fleshing out the concept of authenticate present in the existing UCC definition of signature was thought to be wise. Therefore, the definitional concepts set forth in the prior definition of authenticate have been carried into this definition of signature.

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

Source: UCC Section 1-201(42)
Reporter's Note: This definition has its principal significance in the context of manifestation of assent and opportunity to review. It is bracketed pending the Committee's determination of the status of those concepts in this Act.

(2224) "Transferable record" means a record, other than a writing, that is would be an instrument or chattel paper under [Article 9 of the Uniform Commercial Code] or a document of title under [Article 1 of the Uniform Commercial Code], if the record were in writing.
Source: Oklahoma Model Section II.H.
Textual References: Section 405. Transferable Records.
### Reporter’s Note:
This definition is necessary in the event the Drafting Committee decides to retain the applicability of this Act to such records. See Section 405.

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

**Source:** UCC Section 1-201(46).

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

**Reporter’s Note:** This definition reflects the current UCC definition.

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

- "Basic fact". Section 102(15)
- "Inadvertent error". Section 204
- "Presumed fact". Section 102(15)
- "Relying person". Section 202
- "Requiring party". Section 110
- "Responsible person". Section 202

**Source:** UCC Section 2-103(b).

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

(b) Principles of law and equity shall be used to supplement this [Act] except to the extent that those principles are
[inconsistent with] [displaced by] the terms[, purposes and policies] of a particular provision of this [Act].

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

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

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

Reporter's Note:
1. The scope of the Act has been clarified by limiting its applicability to electronic records and adding electronic signatures. The underlying premise of this section is that this Act applies to all electronic records and signatures unless specifically excluded by the next Section.
2. Notwithstanding the apparent simplicity and clarity of this revised section, the Scope of this Act remains one of the most difficult aspects in the drafting of this Act. At the January meeting it was the view of many observers and members of the Committee, that the attempt to limit scope based on the definition of commercial and governmental transactions was unworkably vague, while at the same time being overly broad (one committee member noted that under the prior draft a secretary in a bank getting a cup of coffee would be covered). In order to achieve clarity and precision, the committee narrowly voted to eliminate the restriction to commercial and governmental transactions. The approach now being taken is to delineate with specificity, in the next section, those transactions and types of transactions which will be excluded.

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

At the May, 1997 meeting, the Drafting Committee expressed strong reservations about applying this Act to all writings and signatures, as is contemplated in the Illinois, Massachusetts and other models. These same reservations were again raised at the September Meeting. The scope section appearing in the last draft
was an attempt to address those concerns by limiting applicability of the Act to only those records and signatures arising in the context of a commercial or governmental transaction, as therein defined. However, the view of a majority of the committee and most observers was that a specific delineation of excluded transactions in the next section was preferable to the attempt to redefine commercial and governmental transactions.

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

SECTION 104. EXCLUDED TRANSACTIONS SUBJECT TO OTHER LAW.

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

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

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

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

(3) [OTHER][such other rules of law as may be designated at the time of the enactment of this Act]].
(c) The provisions of this [Act] and a rule of law referenced in subsection (a) or (b) must be construed whenever reasonable as consistent with each other. If such a construction is unreasonable a rule of law referenced in subsection (a) or (b) governs.

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

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

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

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

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

Source: New

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

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

Reporter's Note:
1. The prior draft reflected comments made at the September, 1997 meeting.

2. The "repugnancy clause" set forth in the prior draft was similar to those appearing in the Mass. and Ill. Acts. The view that such a clause was too ambiguous and impossible to apply was widely shared among both the observers and members of the
Committee. Accordingly, it has been deleted, notwithstanding the view among a few observers and members of the Committee that such a safeguard remains necessary.

3. Subsection (a) will set forth specific areas of law/transaction types to which this Act will not apply. This listing will be developed from the work of the Task Force formed at the January meeting to review statutory compilations in order to identify candidates for exclusion.

SECTION 105. VARIATION BY AGREEMENT.

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

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

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

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

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

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

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

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

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

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

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

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

Source: UCC Section 1-102
Committee Vote: To delete the word underlying Committee 2 Yes -1
No Observers 14 Yes - 2 No

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

The purposes and policies of this Act are:
a) to facilitate and promote commerce and governmental
transactions by validating and authorizing the use of electronic
records and electronic signatures;
b) to eliminate barriers to electronic commerce and
governmental transactions resulting from uncertainties relating
to writing and signature requirements;
c) to simplify, clarify and modernize the law governing
commerce and governmental transactions through the use of
electronic means;
d) to permit the continued expansion of commercial and
governmental electronic practices through custom, usage and
agreement of the parties;
e) to promote uniformity of the law among the states
(and worldwide) relating to the use of electronic and similar
technological means of effecting and performing commercial and
governmental transactions;
f) to promote public confidence in the validity,
integrity and reliability of electronic commerce and governmental
transactions; and

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

SECTION 107. COURSE OF PERFORMANCE, COURSE OF DEALING, AND
USAGE OF TRADE.

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

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

(2) that party performs on one or more occasions;
and
(3) the other party, with knowledge of the nature of the performance and opportunity for objection to it, accepts the performance or acquiesces to it without objection.

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

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

(d) A course of performance or course of dealing between the parties or usage of trade in the vocation or trade in which they are engaged or of which they are or should be aware is relevant in ascertaining the meaning of the parties’ agreement, may give particular meaning to specific terms of the agreement, and may supplement or qualify the terms of the agreement. A usage of trade applicable where only part of the performance under the agreement is to occur may be so utilized as to that part of the performance.
(e) The express terms of an agreement [including terms
to which a party has manifested assent] and any applicable course
of performance, course of dealing, or usage of trade must be
construed wherever reasonable as consistent with each other. If
such a construction is unreasonable:

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

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

(3) course of dealing prevails over usage of
trade.

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

Source: Article 1 Draft Section 1-304.
Committee Vote: To delete this section Committee 5 Yes - 1 No
Observers 16 Yes - 0 No
Reporter's Note: The Committee voted to delete this section
consistent with its policy determination that this Act should be
as strictly procedural in its effect as possible. The view of
the Committee was that the question of usage evidence as
informing the substance of an agreement was an issue best left to
the underlying substantive law of the transaction. Since the
overarching theme of this Act is simply to effectuate an
alternative means to consummate and perform transactions, the
construction of the agreements reached in those transactions is
to be left to the underlying law applicable to the particular
transaction.

The commentary will make clear that the absence of a
provision relating to the employment of usage evidence as a means
of construction is in no way intended to remove such
considerations when otherwise relevant under the substantive law
applicable to the transaction.
[SECTION 1078. MANIFESTING ASSENT. In a transaction governed by this [Act], the following rules apply:

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

(1) signs the record or term or

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

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

(b) The mere retention of information or a record without objection is not a manifestation of assent.

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

(d) A manifestation of assent may be proved in any manner, including by showing that a procedure existed by which a person or an electronic agent must have engaged in conduct or operations
that manifested assent to the record or term in order to proceed further in the transaction.[1]

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

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

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

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

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

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

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

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

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

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

(a) which would calls it to the attention of the a reasonable person and permits review; or

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

Source: Article 2B Draft Section 2B-112(a).
Notes to This Draft: Edited to more closely parallel Article 2B.
Reporter's Note: See Reporter's Note to Section 107, Manifesting Assent, supra.
SECTION 10910. DETERMINATION OF COMMERCIALY REASONABLE SECURITY PROCEDURE; COMMERCIALLY UNREASONABLE SECURITY PROCEDURE; NO SECURITY PROCEDURE.

[ALTERNATIVE 1]

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

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

[ALTERNATIVE 2]

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

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

(1) A security procedure established by law or regulation is commercially reasonable for the purposes for which it was established.
(2) Except as otherwise provided in subsection (b)(1), commercial reasonableness is determined in light of the purposes of the procedure and the commercial circumstances at the time the parties agree to or adopt the procedure.

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

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

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

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

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

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

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

SECTION 110. EFFECT OF REQUIRING A COMMERCIALlY UNREASONABLE SECURITY PROCEDURE.

[ALTERNATIVE 1]

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

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

(2) If the requiring party receives an electronic record or electronic signature purporting to be that of the other party, the requiring party will not be entitled to the benefit of any presumption which may arise under Sections 202, 203 or 302.
(b) A person does not require a security procedure under subsection (a) if it makes commercially reasonable alternative security procedures available to the other person.

[ALTERNATIVE 2]

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

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

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

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

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

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

Source: Alternatives 1 and 2 are both new based on consultation between the Article 2B Reporter and Committee Chair and the UETA Reporter and Committee Chair. Alternative 1 was drafted by the UETA Reporter in consideration of the discussions regarding former section 110(b) at the January meeting. Alternative 2 is from the March, 1998 Draft of Article 2B.
**Reporter's Note:**
General Policy: This section is intended to impose liability and create strong disincentives for the imposition of the use of security procedures which are not commercially reasonable. This section, under either alternative, is intended to apply only in the case where the requiring party is in a position to, and in fact does impose the use of the commercially unreasonable procedure. As noted in subsection (3), if the parties negotiate or jointly select a procedure, or have commercially reasonable alternatives available, this section would have no application. In such a case, or indeed in cases where no security procedure is used, resulting losses are allocated in accordance with the applicable substantive law outside this Act.

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

**Alternative 1 - Structure.**

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

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

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

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

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

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

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

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

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

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

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

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

Illustration 9. Buyer logs on to an internet vendor. In
placing the order it uses a commercially unreasonable
security procedure. Vendor has not agreed to the procedure
but does adopt it by processing the order. This section
does not apply. No presumptions attach since the procedure
was commercially unreasonable, and the parties are left to
deny or prove up the resulting contract.
As indicated by the illustrations, the question of the extent of damage recovery by any party is left entirely to other law. The effect of a commercially unreasonable procedure that is imposed by one party is simply to raise estoppel or deny presumptions. After application of an estoppel, the transaction is proven or denied by other means and the resulting liability determined pursuant to other substantive law.

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

ARTICLE B REPORTER'S NOTES:

Notes to this Draft:
This Section was revised based on consultation with the Electronic Transactions Reporter and Committee chair and in light of the discussion of the issues during the February 1998 meeting.

General Notes:
1. General Policy and Scope. This section deals with allocation of loss in cases where one party (either the licensor or the licensee) requires use of an attribution procedure that is commercially unreasonable and use of that procedure causes a loss either because of undetected errors in transmissions or records or because of third party activity in the nature of fraud or otherwise. The Section does not cover all cases in which such loss might occur, but deals only with circumstances in which a party is in a position to and does in fact require use of the commercially unreasonable procedure. A procedure negotiated or jointly selected by the parties, selected from among alternatives that include a commercially reasonable option, or mutually designed, does not fall within this Section. Responsibility for loss in such cases lies outside this article.
   a. Reliance Loss. The basic premise is that, all things being otherwise equal, loss in the nature of reliance or restitution should fall on the party that required use of the procedure that caused the loss. This is a contract statute, not a general regulatory or tort liability statute and, thus, the losses to which it applies are limited to situations in which loss results from use of the procedure in a transaction to which the requirement applies.
   b. Transactions Not Affected. Additionally, since this entire article deals with licensing and related transactions, the losses are confined to such transactions. The Section does not apply to credit card, funds transfer or other types of transactions in which attribution procedures are used, but which fall outside the scope of Article B and, in many cases, are at least partially regulated by federal or other state laws. Thus, for example, use of an
identifying code for a credit card payment is not governed by this section. However, if a contracting party requires that the other party use a credit card number as an attribution procedure, credit card law applies as to the payment transaction, but as to the contractual relationship, Section B-115 applies if the procedure is regarded as commercially reasonable and this Section applies if the procedure was "required" and is commercially unreasonable.

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

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

The Section does not necessarily create an affirmative right of recovery. In some cases, the Section merely denies the relying party an ability to recover from the other person. Thus, for example, a licensor acting pursuant to a commercially unreasonable attribution procedure, might ship information product to a third party that used the inadequacies of the procedure to dupe the licensor into believing that the party requesting shipment was the named licensee. If the licensor had required the procedure and the licensee had agreed to it for transactions of this type, this Section allows the licensee to resist any effort by the licensor to charge the licensee for the loss or the contract price. The licensor remains responsible.

On the other hand, if the licensee had required the procedure and the licensor agreed to it, the licensor may recover against the licensee for the losses in the nature of reliance. It cannot, of course, in this case seek recovery under contract theory since the licensee did not make the purchase request..

3. Type of Loss. The loss to which this Section applies is limited in several ways.
The loss must, initially, come from use of the procedure. This excludes losses that flow from other, perhaps parallel causes. Thus, if an identifier is unreasonable, but the party actually did engage in the transaction, but suffered loss due to a breach of contract, this section does not apply. The losses addressed here are in the nature of loss from misattribution of who sent a message, tampering with the content of a message, or errors caused by transmission or other factors.

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

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

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

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

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

Illustration 1. S (the vendor) required and M agreed to a procedure for identifying M in placing orders with S. Thief misuses this procedure and, purporting to be M, obtains a $10,000 electronic encyclopedia from S. S, believing that M placed the order, seeks the license fee from M. Under the general attribution sections, if the procedure is not commercially reasonable, there is no presumption that the sender was M and, since M can prove it was not the sender, it has no liability. Under this section, the required attribution procedure caused a loss, but S is responsible for that loss. It cannot shift loss to M.
In some false identity cases, however, the party requiring the use of the attribution procedure may be responsible for affirmative losses.

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

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

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

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

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

Illustration 4[5]. M requires that L use an unreasonable attribution procedure for transmitting orders and acceptances. L agrees and adopts the procedure. It places
an order for ten software widgets. Because the procedure is flawed, the message arrives at M requesting 100 software widgets. M ships on that basis. L desires to ship the ninety excess widgets back to M and not pay. One could argue that no contract exists because of mistake. Alternatively, a contract might be formed on the offer as sent or as received. Case law support exists for either result. This section, however, focuses on reliance loss. Either L or M could be said to suffer loss because of reliance on the procedure. Since M required it, M bears responsibility for the loss. It cannot demand the price for the ninety widgets unless, of course, L decides to accept and retain them. If L had required the use of the procedure, it would be responsible for reliance losses and restitution.

END OF ARTICLE B REPORTER NOTES

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

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

Source: Revised Article 1 Section 1-305 (Sept. 1997 Draft)
Committee Vote: To delete this section Committee Yes 6 - No 1
Observers Yes 7 - No 5
Reporter's Note: This section, added in response to comments at the September Meeting, was deleted by the Committee at the January meeting. The section was viewed as creating substantive requirements best left to the substantive law of the transaction.

SECTION 112. GENERAL PRINCIPLES OF LAW APPLICABLE.

Unless displaced by the particular provisions of this [Act], the principles of law and equity, including the law merchant and the law relating to contract, principal and agent, estoppel, fraud, misrepresentation, duress, coercion, mistake, bankruptcy and other validating and invalidating cause shall supplement its provisions.
**Source:** UCC Section 1-103

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

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

**PART 2**

**ELECTRONIC RECORDS GENERALLY**

**SECTION 201. Leg** **AL RECOGNITION OF ELECTRONIC RECORDS.**

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

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

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

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

**Reporter's Note:**
1. Part 2 reflects the fundamental reorganization of this Act in the November, 1997 Draft. Part 2 now deals with those provisions relating to the validity, effect, and use of electronic records, Part 3 contains those sections dealing with the validity and effect of electronic signatures, and Part 4 reflects general contract provisions, and provisions dealing with the effect of both electronic records and electronic signatures. Under different provisions of substantive law the legal effect and enforceability of an electronic record may be separate from the issue of whether the record contains a signature. For example, where notice must be given as part of a contractual
obligation, the effectiveness of the notice will turn on whether
the party provided the notice regardless of whether the notice
was signed. An electronic record attributed to a party under
Section 202 would suffice in that case, notwithstanding that it
may not contain a signature.

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

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

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

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

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

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

SECTION 202. ATTRIBUTION OF ELECTRONIC RECORD TO A PARTY.

(a) As between the parties, an electronic record is attributable to a party person if:

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

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

(b) Attribution of an electronic record to a party person under subsection (a)(2) has the effect provided for by the agreement regarding the security procedure and, in the absence of terms about such effect, creates a presumption that the electronic record was that of the party person to which it is attributed.
Even if an electronic record is not attributable to a person under subsection (a), a person ("responsible person") is liable for losses in the nature of reliance, if the losses occur because the electronic record:

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

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

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

(4) the use of the access numbers, codes, computer programs or the like created the appearance that the electronic record came from the party responsible person.

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

(i) The relying party has the burden of proving reasonable reliance, and the party to which the electronic record is to be attributed has the burden of proving reasonable care.
(2) Reliance on an electronic record that does not comply with a security procedure is not reasonable unless authorized by an individual representing the party to which the electronic record is to be attributed.

Source: Article B Draft Section B-116.

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

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

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

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

Subsection (c) is part of the March Draft of Article 2B but has been bracketed here for the Committee's consideration. In substance it appeared as subsection (a)(3) in the prior drafts of both this act and Article 2B, with the result that in the case of negligence an electronic record could be attributed to, and therefore binding upon, a party. The substance of this subsection does not truly address the issue of attribution and has been properly set off as a separate basis for liability. It is more in the nature of a direct loss allocation provision rather than an attribution provision. Under subsection (c) when the negligence of one party, together with reasonable reliance by the other party caused by the negligence, results in loss to the relying party, the negligent party bears losses "in the nature of reliance." Like Alternative 2 to Section 110 regarding the effect of requiring a commercially unreasonable security procedure, this section implicates substantive loss allocation
determinations. Considering the Committee's apparent desire to avoid such substantive effects, it may be possible to redraft this subsection along the lines of Alternative 1 to Section 110.

SECTION 203. DETECTION OF CHANGES AND ERRORS.  

(a) If through a security procedure to detect errors or changes in the informational content of an electronic record, between the parties the following rules apply:

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

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

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

       (1) If the sender complied with the security procedure, but the other party did not, and the change or error would have been detected had the receiving other party also complied with the security procedure, the sender is not bound by the error or change.
(d)(2) If the sender receives a notice the other party notifies the sender in a manner required by the security procedure that describes the informational content of the record as received, the sender shall review the notification and report any error detected by it in a commercially reasonable manner. Failure to so review and report any error shall bind the sender to the informational content of the record as received.

Source: Article 2B Draft Section 2B-117
Notes to this Draft: Edited for clarity and to more closely track Article B.

Reporter's Note:
1. Like Section 202, 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. Again, since the parties will have agreed or adopted the security procedure, the creation of the presumption of accuracy, and allocation of risk to the party that should have discovered the error, should not pose undue hardship or unfair surprise on the party bearing the loss.

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

(bc) In an automated transaction involving an individual, the individual is not responsible for an electronic record that the individual did not intend but that was caused by an inadvertent error if, on learning of the other party's reliance on the erroneous electronic record, the individual:
(1) in good faith promptly notifies the other party of the error and that the individual did not intend the electronic record received by the other party;

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

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

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

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

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

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

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

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

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

SECTION 2054. ORIGINALS: ACCURACY OF INFORMATION ACCURACY.

(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 for if the record is not being presented or retained in its original form, that requirement is met by an electronic record if [the electronic record is shown to reflect accurately] [there exists a reliable assurance as to the integrity of] the information set forth in the electronic record from the time when 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 that arises 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.

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

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

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

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

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

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

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

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

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

SECTION 2065. RETENTION OF ELECTRONIC RECORDS.

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

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

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

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

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

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

(d) Nothing in this section does not preclude any federal
or state agency from specifying additional requirements for the
retention of records, either written or electronic, subject to
the agency's jurisdiction.

Source: Uncitral Model Article 10; Illinois Model Section 206.
Reporter's Note: At the May meeting concern was expressed that
retained records may become unavailable because the storage
technology becomes obsolete and incapable of reproducing the
information on the electronic record. Subsection (a)(1)
dresses this concern by requiring that the information in the
electronic record "remain" accessible, and subsection (a)(2)
dresses the need to assure the integrity of the information
when the format is updated or changed.

This section would permit parties to convert original
written records to electronic records for retention so long as
the requirements of subsection (a) are satisfied. Accordingly, in
the absence of specific requirements to retain written records,
written records may be destroyed once saved as electronic records
satisfying the requirements of this section.
PART 3

ELECTRONIC SIGNATURES GENERALLY

SECTION 301. LEGAL RECOGNITION OF ELECTRONIC SIGNATURES.

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

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

(b) In any transaction, a party may establish reasonable requirements regarding the method and type of signatures which will be acceptable to it.

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

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

2. Subsection (b) is a particularized application of Subsection (a). Its purpose is to validate and effectuate electronic signatures as the equivalent of pen and ink signatures, subject to all of the rules applicable to the efficacy and formality of a signature, except as such other rules are modified by the more specific provisions of this Act.
3. This section, consistent with the existing UCC definition of a signature as "any symbol executed or adopted by a party with present intention to authenticate a writing," merely reiterates for clarity the rule that an electronic record containing an electronic signature satisfies legal requirements. The critical issue in either the signature or electronic signature context is what the signer intended by the execution, attachment or incorporation of the signature into the record.

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

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

SECTION 302. ELECTRONIC SIGNATURES: EFFECT AND PROOF.

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

(1) the signing party's identity

(2) its adoption and acceptance of a record or a term

and

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

(b) If the signing party executed or adopted the an electronic signature is executed or adopted in accordance with a
commercially reasonable security procedure for validating electronic signatures, the following rules apply:

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

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

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

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

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

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

Source: Article 2B Draft Section 2B-118(a and c); Illinois Model Section 203.
Committee Vote: To delete subsection (c) but retain its effect as a presumption. Committee Unanimous in favor - Observers 14 Yes - 2 No
Reporter's Note:
1. An electronic signature is any symbol or methodology adopted with intent to sign a writing. This Act includes in the definition of signature the attributes normally associated with a pen and ink signature in order to make clear what a signer intends by signing a document, i.e., to identify oneself, adopt the terms of the signed record, and verify the integrity of the informational content of the record which is signed. By identifying the multi-purpose effect of a signature, this Act clarifies the assumption as to the intent of one signing any record. Subsection (a) simply applies this assumption to the electronic signature. As with a signature on paper, the signing party remains free to prove that the signing was intended to accomplish only 1 or 2 of the normal purposes associated with a signing.

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

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

4. Former subsection (c) has been deleted consistent with the Committee's instructions. The substantive effect has been moved to subsection (b) by creating a presumption of authority and authenticity where a commercially reasonable security has been used. Unless the validity of an electronic signature is denied by the purported signer, the presumption will stand to establish the authority and authenticity of the electronic signature. However, if the purported signer denies the validity of the signature, the presumption would be overcome, and the party asserting validity must carry the burden of so establishing.
SECTION 303. [SIGNATURES BY] [OPERATIONS OF] ELECTRONIC AGENTS.

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

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

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

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

2. This section extends signing to the electronic agent, automated context. 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 (i.e., with present human intent to authenticate the electronic record), 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 bound and deemed to have signed the records of the electronic agent.

PART 4

ELECTRONIC CONTRACTS AND COMMUNICATIONS

SECTION 401. FORMATION AND VALIDITY.

(a) Unless otherwise agreed, if an electronic record is used in the formation of a contract, the contract may not be denied legal effect, validity or enforceability solely because
on the sole ground that an electronic record was used for that purpose.

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

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

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

(2) A contract may be formed by the interaction of an electronic agent and an individual. A contract is formed by such interaction if (A) the individual has reason to know (i) that the individual is dealing with an electronic agent and (ii) the limitations on the ability of the electronic agent to react to contemporaneous expressions by the individual and (B) the individual performs actions that the individual knows or reasonably should know will cause the electronic agent to complete the transaction or performance or permit further use, or that which are clearly indicated as constituting acceptance, regardless of other expressions or actions by the individual to
which the individual cannot reasonably expect the electronic
agent to react.

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

(A) terms of the parties' agreement (including terms
with respect to which either party has manifested assent);

(b) terms that the electronic agent could take into
account and;

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

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

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

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

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

Source: Article 2B Draft Section 2B-204; Uncitral Model Article
11.
Committee Vote: To delete the concept of manifestation of assent from Subsection (b)(3) (former subsection (c)(3)) Committee 6 Yes - 0 No Observers 15 Yes - 0 No

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

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

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

As noted in a number of comments at the January meeting, whether one knows that one is dealing with an electronic agent should be irrelevant, so long as the individual proceeds with actions it knows or reasonably should know will result in accomplishment of the ends desired. Concerns previously expressed by observers that individuals may not know what contemporaneous statements made by the individual would be given effect because of the possibility of contemporaneous or subsequent human review, have been addressed by limiting those actions of the individual which may result in a contract to those which the individual would reasonably expect to result in a contract. This will provide the party employing an electronic agent with an incentive to make clear the parameters of the agent's ability to respond. If the party employing the electronic agent provides such information, the individual's act of proceeding on the basis of contemporaneous actions or expressions not within the parameters of the agent would be unreasonable and such actions and expressions could not be the basis for contract formation.
4. Finally, subsection (c) deals with timing in the formation of a contract by electronic means. Subsection (c)(2) makes clear that acceptance by performance, either in whole or in part, when the performance is electronic, occurs on receipt. When acceptance of an offer by performance occurs other than electronically (e.g. by the shipment of product), acceptance is governed by other rules of law such as the UCC and common law. As to timing of receipt see section 402.

SECTION 402. TIME AND PLACE OF SENDING AND RECEIPT.

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

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

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

(d) Unless otherwise agreed between the sender and the recipient, an electronic record is deemed to be sent from where the sender has its place of business and is deemed to be received
where the recipient has its place of business. For the purposes of this subsection:

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

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

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

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

Reporter's Note:

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

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

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

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

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

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

SECTION 403. ELECTRONIC ACKNOWLEDGMENT OF RECEIPT.

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

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

(2) If the sender requests electronic acknowledgment but does not state indicate that the record is conditional on electronic acknowledgment, and does not specify a time for receipt, and electronic acknowledgment is not received within a reasonable time after the record is sent, the sender, upon notifying the other party, may either
(A) treat the record as having expired no longer effective; or

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

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

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

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

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

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

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

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

SECTION 404. ADMISSIBILITY INTO EVIDENCE.

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

(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 information or circumstances.

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

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

Nothing in this section relieves a party from establishing the necessary foundation for the admission of an electronic record. Subsection (b) gives guidance to the trier of fact in according weight to otherwise admissible electronic evidence.
SECTION 405. TRANSFERABLE RECORDS. If the identity of the rightful holder of person entitled to enforce a transferable record can be reliably determined from the record itself or from a method employed for recording, registering, or otherwise evidencing the transfer of interests in such records, the rightful holder of person entitled to enforce the record is considered deemed to be in possession of the record.

Source: Oklahoma Model Section III.B.2.

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

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

PART 5

GOVERNMENTAL ELECTRONIC RECORDS

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

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

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

Reporter’s Notes: See Notes following Section 504.
SECTION 502. RECEIPT AND DISTRIBUTION OF ELECTRONIC RECORDS BY
GOVERNMENTAL AGENCIES.

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

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

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

(2) if electronic records must be electronically signed, the type of electronic signature required, and the manner and format in which the electronic signature must be affixed to the electronic record, and the identity of, or criteria that must be met by, any third party used by a person filing a document to facilitate the process;
(3) control processes and procedures as appropriate to ensure adequate integrity, security, confidentiality, and auditability of electronic records; and

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

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

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

(de) Nothing in this [Act] may be construed to require any state governmental agency to use or permit the use of electronic records or electronic signatures.

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

Reporter's Note: See Notes following Section 504.

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

The [designated state officer] may adopt regulations setting forth rules, standards, procedures and policies for the use of electronic records and electronic signatures by governmental
agencies. Where appropriate, such regulations shall specify differing levels of standards from which implementing governmental agencies can choose in implementing the most appropriate standard for a particular application.

Source: Illinois Model Section 802(a).
Reporter's Note: See Notes following Section 504.

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

Source: Illinois Model Section 803.

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

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

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

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

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

4. Section 504 requires regulating authorities to take account
of consistency in applications and interoperability to the extent
practicable when promulgating regulation. This section is
critical in addressing the concerns of many at our meetings that
inconsistent applications may promote barriers greater than
currently exist.
PART 6

MISCELLANEOUS PROVISIONS

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

Source: Article 1 Draft Section 1-106.

SECTION 602. EFFECTIVE DATE.

Source:

SECTION 603. SAVINGS AND TRANSITIONAL PROVISIONS.

Source: