Law, Practice, and Policy at the Bleeding Edge—2017 Technology Law Updates

Cosponsored by the Technology Law Section

Thursday, October 5, 2017
8:45 a.m.–12:30 p.m.

2.5 General CLE credits and 1 Ethics credit
SECTION PLANNERS

Leigh Gill, Immix Law Group PC, Portland
Robert Swider, Swider Haver LLP, Portland
Ellen Taussig Conaty, Department of Justice General Counsel Transactions, Salem
Laura Zager, Attorney at Law, Portland

OREGON STATE BAR TECHNOLOGY LAW SECTION EXECUTIVE COMMITTEE

Leigh Francis Gill, Chair
Travis J. Benn, Chair-Elect
Scott Schneider, Past Chair
Marinus Damm, Treasurer
Dave Bourgeau, Secretary
Nicholas F. Aldrich
Chad M. Colton
Aaron J. Cronan
Andrea Hicks Jasinek
Tricia Juettemeyer
Jesse Lev London
Robert A. Swider
Ellen D. Taussig Conaty
Marc Visnick
Alexander James Wall
Laura A. Zager

The materials and forms in this manual are published by the Oregon State Bar exclusively for the use of attorneys. Neither the Oregon State Bar nor the contributors make either express or implied warranties in regard to the use of the materials and/or forms. Each attorney must depend on his or her own knowledge of the law and expertise in the use or modification of these materials.

Copyright © 2017

OREGON STATE BAR
16037 SW Upper Boones Ferry Road
P.O. Box 231935
Tigard, OR 97281-1935
### TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Schedule</th>
<th>v</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faculty</td>
<td>vi</td>
</tr>
</tbody>
</table>

1. **Technology on Contracting: Practical and Legal Implications** 1–i  
   — Aaron Cronan, *Cronan Law LLC, Portland, Oregon*

2. **Strategies for Commercialization of Technology Startup Funding—Presentation Slides** 2–i  
   — Ken Vaughn, *Oregon BEST, Portland, Oregon*

   — Serena Morones, *Morones Analytics LLC, Portland, Oregon*  
   — Jennifer Murphy, *Morones Analytics LLC, Portland, Oregon*

4. **Where’s Your Data? Data Privacy and Your Ethical Obligations** 4–i  
   — Calon Russell, *Holland & Knight LLP, Portland, Oregon*  
   — Dayna Underhill, *Holland & Knight LLP, Portland, Oregon*
SCHEDULE

8:00  Registration

8:45  Technology on Contracting: Practical and Legal Implications
  ➤ Technologies used during the contracting process
  ➤ Benefits and pitfalls of e-signing
  ➤ Collaboration via Google Docs and e-mail
  ➤ Best practices for PDF usage
  Aaron Cronan, Cronan Law LLC, Portland

9:45  Strategies for Commercialization of Technology Startup Funding
  ➤ Raising capital from angel investors
  ➤ Business structures
  ➤ Funding vehicles
  ➤ Startup challenges
  Ken Vaughn, Oregon BEST, Portland

10:30 Break

10:45  Data Visualization: How Your Expert Can Help You Tell Your Story
  ➤ Taking your case from produced data to data visualization
  ➤ Oregon’s 2013 big tobacco case
  Serena Morones, Morones Analytics LLC, Portland
  Jennifer Murphy, Morones Analytics LLC, Portland

11:30 Where’s Your Data? Data Privacy and Your Ethical Obligations
  ➤ Sources and causes of data breaches
  ➤ Ethical rules related to data security
  ➤ Appropriate protective measures and best practices
  ➤ Responding to a data breach
  Calon Russell, Holland & Knight LLP, Portland
  Dayna Underhill, Holland & Knight LLP, Portland

12:30 Adjourn
**FACULTY**

**Aaron Cronan,** *Cronan Law LLC, Portland.* Mr. Cronan focuses on helping clients start businesses, file trademarks, and negotiate contracts and licensing. He also specializes in helping firms and companies handle complex e-discovery issues. He is admitted to practice law in Oregon and California.

**Serena Morones,** *Morones Analytics LLC, Portland.* Ms. Morones specializes in forensic accounting, damage analysis, and business valuation. She has helped lead numerous large and complex litigation cases to financial resolution through settlement or expert testimony. Ms. Morones serves as an independent expert to assist parties in settling valuation or economic disputes. Ms. Morones has practiced through her own firm since 2002 and began her forensic accounting/valuation specialty in 1996.

**Jennifer Murphy,** *Morones Analytics LLC, Portland.* Ms. Murphy provides expert services in financial damage analysis, forensic accounting, fraud investigation, and business valuation. As the Managing Director of Morones Analytics, she leads the firm’s quality control review processes. Ms. Murphy also serves as the firm’s primary expert in the areas of data analytics and lost earnings damage analysis. Ms. Murphy has over 20 years of professional accounting experience.

**Calon Russell,** *Holland & Knight LLP, Portland.* Mr. Russell advises lawyers, law firms, and government and corporate legal departments on legal ethics and professional responsibility matters. His practice involves assisting clients at the organizational level with law firm formation and operations, dissolution, and lateral lawyer moves. He also counsels on regulatory compliance issues such as the unauthorized practice of law, litigation financing, fee splitting, conflicts of interest, and state bar admissions. As part of his practice, Mr. Russell also focuses on civil litigation, primarily at the appellate level, and has a background in constitutional law, labor and employment matters, construction defect litigation, foreclosure proceedings, premises liability, and the representation of public officials. He is a member of the Multnomah Bar Association.

**Dayna Underhill,** *Holland & Knight LLP, Portland.* Ms. Underhill focuses her practice on complex commercial litigation, as well as legal ethics and risk management for law firms, lawyers, and corporate in-house counsel. She advises lawyers on all aspects of the law governing lawyers, including the defense of bar disciplinary complaints, lawyer mobility, lateral hiring, client engagement, conflicts of interest, attorney-client privilege, and law firm data privacy, breach, and response. Ms. Underhill also maintains an active state and federal court employment and complex commercial litigation practice. She is a member of the Oregon State Bar House of Delegates, Oregon Women Lawyers, the Washington State Bar Association Disciplinary Advisory Roundtable, the Association of Professional Responsibility Lawyers, and the American Bar Association Labor and Employment Section and Center on Professional Responsibility. She is a frequent speaker on all aspects of the law governing lawyers. As an adjunct professor at Lewis & Clark Law School, Ms. Underhill taught trial practice and coached the law school mock trial team at the American College of Trial Lawyers National Competition for two consecutive years.

**Ken Vaughn,** *Oregon BEST, Portland.* As Director of Commercialization Programs for Oregon BEST, Mr. Vaughn manages the programs that provide grants to researchers at Oregon’s state universities and make investments in Oregon startup companies. These programs are designed to accelerate research and technology development to remove the barriers to customer adoption and follow-on investments by private investors. He collaborates with innovators, investors, mentors, support organizations, and senior management talent to help assemble the elements necessary for launching a successful business in the cleantech sector in Oregon. Before joining Oregon BEST, he held senior management positions in engineering, product management and marketing in a wide range of industries. He has experience in managing innovation, starting companies, advising early-stage companies, and investing in early-stage ventures.
Chapter 1
Technology on Contracting: Practical and Legal Implications

Aaron Cronan
Cronan Law LLC
Portland, Oregon

Contents

Presentation Slides ......................................................... 1–1
Uniform Electronic Transactions Act (1999) ......................................................... 1–47
ORS Chapter 84—Electronic Transactions ............................................... 1–113
Technology on Contracting: Practical and Legal Implications

How I Learned to Stop Worrying and Love the Machines

- Graduated UC Hastings 2000
- End of book research
- Ground Zero of Dot Bomb
- 1st Firm – Attorney Computers 2002
How I Learned to Stop Worrying and Love the Machines

- Peer file sharing

- Electronic Discovery Consulting
  - Email and/or text in every case
  - Data preservation and collections

- 80% Virtual Law Office

Course Overview

- Digital Impact
- Electronic Signatures
- Legislation – E–Sign, UETA
- Statute of Frauds
- Email Signatures
- Assent – Clickwrap
- Contract Drafting – Redlining, AI Review, Finalizing, Collaborating (Google Docs)
- Signing – Paper, Electronic
- Conclusion – Golden Age of Contracts
Digital Impact

› Electronic communications
  ◦ Increased ease and volume
  ◦ Changes in formation
  ◦ Changes in signing
  ◦ Changes in terms and scope
  ◦ Written Record

Digital Impact

› Electronic Transactions
  ◦ E-signing
  ◦ Statute of Frauds
  ◦ Assent – Clickwrap/Browserwrap
Electronic Signature

- E-Signing is Valid!
- Federal E-signatures law – 17 years old
- Much Better Authentication
“[T]here is no benefit to any party to an electronic transaction, with very few exceptions, in requiring that they be memorialized on paper with signatures that are manual.”

Legislation – E-Sign

› Electronic Signatures in Global and National Commerce Act ("E-Sign") – 2000
› 15 U.S.C. § 7001
  ◦ Signature – “may not be denied validity solely because it is in electronic form” Id.
  ◦ Electronic Signature – "an electronic sound, symbol or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." Id. § 7006(5)

Legislation – E-Sign

› High Lights:
  ◦ Not required to accept e-signatures
    • But you should
  ◦ Accurate electronic copies are valid (§ 7001 (d))
Legislation – E-Sign

- Electronic Agents can form contract (§ 7001 (h))
- “Electronic Agent” is hereinafter “Robot”
- Robots can form contracts

Legislation – E-Sign

- Notary can be signed electronically (§ 7001 (g))
  - Still have to be in person
Legislation – UETA

- Uniform Electronic Transactions Act (UETA) 1999
  - Expressly validates electronic records, signatures and contracts.

Legislative Enactment Status
Electronic Transactions Act

Generated on Saturday, July 22, 2017, 7:20 PM
Legislation – UETA

Oregon UETA 2001

ORS 84.001

Partially supersedes Federal E-Sign

ORS 84.007 SCOPE.

(1) Applies to electronic records and electronic signatures relating to a transaction.

(2) Does not apply to:

(a) wills, codicils, or testamentary trusts;

(b) The Uniform Commercial Code other than Sections 1-107 and 1-206, Article 2, and Article 2A;

(c) the Uniform Computer Information Transactions
ORS 84.013. USE OF ELECTRONIC RECORDS AND ELECTRONIC SIGNATURES

- (1) Does not REQUIRE electronic means
- (2) Parties MUST agreed to conduct transactions by electronic means.
  - Determined from the context and surrounding circumstances, including the parties’ conduct.

ORS 84.019. LEGAL RECOGNITION OF ELECTRONIC RECORDS, SIGNATURES, AND CONTRACTS.

- Cannot be denied legal effect solely because electronic form:
  - (1) Records, signatures
  - (2) Contracts
  - (3) Writings
  - (4) Electronic signature
  - (distinction see UETA comments section 7)
Illustration 1: Email
A to B: “I hereby offer to buy widgets from you, delivery next Tuesday. /s/ A.”

B to A: “I accept your offer to buy widgets for delivery next Tuesday. /s/ B.”

Illustration 1: Email
May not be denied effect solely because they are electronic.
Emails do qualify as records under the Statute of Frauds. (Discussed Later)
But, no quantity stated – unenforceable under UCC Section 2-201(1).
Legislation – UETA

› Illustration 2: Emails

› A to B: “I hereby offer to buy 100 widgets for $1000, delivery next Tuesday. /s/ A.”

› B to A: “I accept your offer to purchase 100 widgets for $1000, delivery next Tuesday. /s/ B.”

Legislation – UETA

› Illustration 2: Emails

› Same analysis as Ill #1

› Now emails also satisfy UCC 2–201(1).
84.025. ATTRIBUTION AND EFFECT OF ELECTRONIC RECORD AND ELECTRONIC SIGNATURE.

- (1) E-signature is attributable to a person if it was the act of the person.

- (2) Determined from the context and surrounding circumstances at the time of its creation, execution, or adoption.

Change or error in an electronic record occurs:

- (1) A party conforming to security measure may avoid an error that the non-conforming party could/should have detected.

- (2) Human v. Robot (electronic agent) the human error can be avoided if the robot did not provide an opportunity for correction and the human:
  - (A) promptly notifies the robots master of the error;
  - (B) takes reasonable steps to return or destroy the consideration. and
  - (C) has not used or received any benefit or value from the consideration.

- (3) If neither (1) nor (2) applies, apply other law, including the law of mistake, and the contract.

- (4) Paragraphs (2) and (3) may not be varied by agreement.
ORS 84.034. RETENTION OF ELECTRONIC RECORDS; ORIGINALS.

- (1) Record retention laws are satisfied by electronic record that:
  - (1) accurately reflects the information set forth in the record after it was first generated in its final form; and
  - (2) remains accessible for later reference. (Must migrate from legacy systems)

- (6) Law requiring record be presented or retained in its original form is satisfied if (1) is satisfied.
ORS 84.037. ADMISSIBILITY IN EVIDENCE.

“In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.”

SECTION 14. AUTOMATED TRANSACTION.

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

(1) A contract may be formed by the interaction of [Robots] of the parties, even if no [human] was aware of or reviewed the [Robots’] actions or the resulting terms and agreements.”
Legislation – UETA

- ORS 84.040. AUTOMATED TRANSACTION.
- Robot v. Robot transactions
- Examples:
  - Computer stock trades
  - Smart appliances (Freezer ordering groceries, printer ordering ink)
  - Smart Contract – Blockchain
- Issues:
  - Unintended action
  - Failure to act

Comment: When robots are involved, the requisite intention flows from the programing and intent to use the robots.
ORS 84.040. AUTOMATED TRANSACTION. (con’t)

(2) Human and Robot can form a contract including when:
   ◦ the human performs actions it is free to refuse to perform and,
   ◦ the human knows or has reason to know will cause the robot to complete the transaction.

Examples:
   ◦ Online purchases
   ◦ Clicking “I accept” Terms of Use
ORS 84.043. TIME AND PLACE OF SENDING AND RECEIPT.

- **Time**
  - (1) Electronic record is sent when it:
    - (a) is addressed properly to, recipient’s designated IP system and can be retrieved;
    - (b) is correctly formatted for that system; and
    - (c) enters an IP system outside the control of the sender.
  - (2) Electronic record is received when it:
    - (a) enters an recipient’s designated IP system and can be retrieved; and
    - (b) is correctly formatted for that system.

- **Place**
  - (4) Electronic record is deemed to be sent from the sender’s place of business and to be received at the recipient’s place of business.
Why Place of Business Matters

- Email sent from hotel or home
- Physical servers bear no relationship to the parties’ locations or intentions

(e) An electronic record is received even if no individual is aware of its receipt.

- Note: paper analog, recipient who never reads a mail notice.
E-Mailbox Rule

- Mail Box Rule:
  - Offer by mail is not effective until received by the offeree.
  - Acceptance is effective as soon as it is posted.
  - Revocation must be received by the offeree before posting letter of acceptance.

- Email and the Mailbox Rule (con’t)
  - Generally, acceptance is effective when sent, regardless of whether it reaches the offeror. See Restatement (2nd) § 63.
  - A contract is created upon mailing of the acceptance regardless of [when / whether] the acceptance was received. Oregon UCJI 65.16
E-Mailbox Rule

- Email and the Mailbox Rule (con’t)
  - Mild trend: Rebuttable presumption that emails are received once sent.
    - American Boat Company v. Unknown Sunken Barge 418 F.3d 910 (8th Cir. 2005)
    - Tinder v. Pinkerton Sec., 305 F.3d 728, 735–36 (7th Cir. 2002)

Statute of Frauds

- British Parliament in 1677
  - Clearly relevant in 2017
- Contracts that must be in writing, and
- Subscribed by the party to be charged:
  - 1) contracts for the sale of an interest in land,
  - 2) contracts for the sale of goods for $500 or more (under the U.C.C.),
  - 3) contracts in consideration of marriage,
  - 4) contracts that cannot be performed within one year of the contract being made and,
  - 5) contracts of suretyship.
Statute of Frauds

› **Writing** is the easy part.
  ◦ **ORS 41.570 – Writings:**
  ◦ Contracts made by telegraph; and
  ◦ All communications sent by telegraph, and signed by the sender, or by the authority of the sender

  ◦ NY Code § 5–701(b)(4) “the tangible written text produced by telex, telefacsimile, computer retrieval or other process by which electronic signals are transmitted by telephone or otherwise shall constitute a writing . . .”

Statute of Frauds

› **Signatures** is where the conflict lives

› But the UETA and E–Sign resolve the issue, right?
Email Signatures

Electronic Signature – “an electronic sound, symbol or process, attached to or logically associated with a contract … and executed or adopted by a person with the **intent to sign the record.**” E-Sign § 7006(5)

Dear Adam, I want to buy your house for $600,000. No contingencies.

/s/ Betty Balm

Betty B. Balm
555.555.5555
Email Signatures

Dear Betty, That sounds good. Let’s do it.

/s/ Adam Allen

Adam A. Allen
555.555.4444

Email Signatures

Dear Adam, I want to buy your house house for $600,000. No contingencies.

Betty Balm

Betty B. Balm
555.555.5555
Email Signatures

Dear Betty, That sounds good. Let’s do it.

Adam A. Allen
555.555.4444
Email Signatures

Dear Betty, That sounds good. Let’s do it.

Adam

Email Signatures

Dear Betty, That sounds good. Let’s do it.

–A
Email Signatures

Dear Betty, That sounds good. Let’s do it.

;-P

Email Signatures

› East v. West
› California
› Merely signing one’s name at the bottom of an e-mail is far from sufficient to bind that person in contract, let alone to a settlement agreement.

Email Signatures

- California’s Uniform Electronic Transactions Act
- Enforcing party must show:
  1) the parties agreed to conduct an electronic transaction and
  2) the signing party wrote his or her name on the email with the intent to formalize an electronic transaction

Email Signatures

- Massachusetts

- Emails typed and sent by defendant containing a salutation consisting of defendant’s name can constitute writings sufficient to satisfy the statute of frauds.
Chapter 1—Technology on Contracting: Practical and Legal Implications

Email Signatures

- New York

“The sender manifested his intention to authenticate the email for purposes of the Statute of Frauds by typing his name, ‘Denis’ at the bottom of the January 12, 2007 email referencing the parties’ ‘contractual agreement’…”


Email Signatures

- Fact Dependent
- State Dependent
- Get express assent and some indication of signing intent
- Don’t leave anything to chance
Assent

› Browserwrap – Terms of Use – Constructive notice (Arbitration Clause)
  ◦ *Nguyen v Barnes & Noble, Inc.*, 763 F.3d 1171 (9th Cir. 2014) – Terms of Use link on every page without more was insufficient notice of terms to imply assent.

Assent

› Clickwrap – Manifest assent – “I Agree” check box
  ◦ Varying enforceability
  ◦ Contract of Adhesion
  ◦ Factors:
    ◦ Are the terms actually visible when clicking?
    ◦ Are terms within reasonable expectations?
    ◦ Is there mutuality for a term?
Assent

- **Clickwrap**
- **Second Life**

- **Included in the TOS:**
  - California choice of law
  - Forum selection
  - Arbitration
  - Confidentiality

---

Assent

- **Clickwrap**
- **Second Life**

- **Applied California Unconscionability Law:**
  - oppression through unequal bargaining positions or,
  - surprise through hidden terms common in the context of adhesion contracts. And;
  - overly harsh or one-sided results that “shock the conscience.”
Assent

› **Clickwrap**

› **Second Life (con’t)**

› **Support Unconscionable Finding:**
  ◦ Arbitration cost advance greater than court filing.
  ◦ Forum selection clause given unequal circumstances.
  ◦ Confidentiality clause.

Assent

› **Clickwrap**

› **Clickwrap TOS = 😞**
  ◦ Waste of time
    • 76 days to read all terms
    • $781 billion US opportunity cost

  • https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/
Clickwrap

- No one reads them
- Horrible or unexpected terms
Confidential Information. Each party (the "Recipient") agrees to protect the Confidential Information of the other party (the "Disclosing Party") in a manner consistent with the treatment that Recipient accords its own Confidential Information of a similar nature, and the Recipient agrees to use and reproduce Confidential Information only to perform its obligations under this Agreement, for the discussion and/or evaluation of potential transactions, or for its internal collection, analysis, and planning purposes. The Recipient may disclose Confidential Information to its employees, agents, and subcontractors, who have a need to know, and employees of any legal entity that it controls, controls it, or with which it is under common control, who have a need to know. The Recipient shall be liable for any use, disclosure or dissemination of Confidential Information by such persons. Confidential Information is any information which is identified by the Disclosing Party at the time of disclosure as being of a confidential nature (including, but not limited to, business plans, products, trade secret processes or methodologies, software, documentation, design specifications, other technical documents and other proprietary rights or information) or that is disclosed to the Recipient under circumstances that would lead a reasonable person to understand that such information is confidential or proprietary in nature. Confidential Information does not include information that (i) is or becomes generally available to the public without breach by Recipient of its confidentiality obligations under this Agreement, (ii) is received by Recipient from a third party without restriction against disclosure, (iii) was known to Recipient without restriction against disclosure prior to disclosure by Disclosing Party, (iv) was independently developed by Recipient without subsequent use of Disclosing Party’s Confidential Information or (v) Recipient becomes legally compelled (including by any investigative demand or similar process) to disclose any of the Confidential Information. If Recipient becomes legally compelled to disclose any of the Confidential Information, Recipient shall (to the extent legally permitted) provide Disclosing Party with prompt prior notice of such requirement so that Discloser may seek a protective order or other appropriate remedy.

Confidential Information. Each party (the "Recipient") agrees to protect the Confidential Information of the other party (the "Disclosing Party") in a manner consistent with the treatment that Recipient accords its own Confidential Information of a similar nature, and the Recipient agrees to use and reproduce Confidential Information only to perform its obligations under this Agreement, for the discussion and/or evaluation of potential transactions, or for its internal collection, analysis, and planning purposes. The Recipient may disclose Confidential Information to its employees, agents, and subcontractors, who have a need to know, and employees of any legal entity that it controls, controls it, or with which it is under common control, who have a need to know. The Recipient shall be liable for any use, disclosure or dissemination of Confidential Information by such persons. Confidential Information is any information which is identified by the Disclosing Party at the time of disclosure as being of a confidential nature (including, but not limited to, business plans, products, trade secret processes or methodologies, software, documentation, design specifications, other technical documents and other proprietary rights or information) or that is disclosed to the Recipient under circumstances that would lead a reasonable person to understand that such information is confidential or proprietary in nature. Confidential Information does not include information that (i) is or becomes generally available to the public without breach by Recipient of its confidentiality obligations under this Agreement, (ii) is received by Recipient from a third party without restriction against disclosure, (iii) was known to Recipient without restriction against disclosure prior to disclosure by Disclosing Party, (iv) was independently developed by Recipient without subsequent use of Disclosing Party’s Confidential Information or (v) Recipient becomes legally compelled (including by any investigative demand or similar process) to disclose any of the Confidential Information. If Recipient becomes legally compelled to disclose any of the Confidential Information, Recipient shall (to the extent legally permitted) provide Disclosing Party with prompt prior notice of such requirement so that Discloser may seek a protective order or other appropriate remedy.
Drafting – Redline

- Redline Tips
  - Ask for MS Word over PDF
  - Expressly require track changes
  - Activate track changes and save before emailing
  - Comparison Tool in a pinch
  - Emails create change record

Drafting – Review Automation

- Contract Artificial Intelligence
  - Deep learning review
  - Compare common language for deviation
  - Preapprove acceptable terms
  - Establish playbook/template
Drafting – Finalizing

- **Finalizing Tips**
  - Final draft – email Word redline and clean PDF
  - Always execute with PDF
    - Printing consistency
    - Security
  - Always Lock PDF
    - Restrict Editing (keeps searchable text) or
    - Print to Image (flattens image, not searchable)
    - (File > Print, click Advanced, check “Print as Image”)

Drafting – Google Docs/Drive

- **Pros:**
  - Great Client Collaboration
  - History of all changes and comment
  - Comment threads in document
  - No emailing drafts
  - Notification of changes
  - Similar to Word
  - Export into other formats (Word, PDF)
Drafting – Google Docs/Drive

Cons:
- Not designed for lawyers
  - File ownership/control
  - Folder Structure
  - No set version control & fixed revisions
- Change history shows date & time of changes
- Constant notification of changes
- Not exactly like Word
- Exporting formatting can be messy

Google Drive – Tips:
- Make it yours
  - Make a copy to your own client folder
  - Share it with only the necessary client contacts
  - Verify who has access and editing privileges
  - Turn off editing and access when done
- Use the comment tool
  - Discuss specific issues until marked resolved
Drafting – Google Docs/Drive

Google Drive – Tips:

- Require clients use tracks changes!
  - Suggestion Mode
- Version Control
  - Create discrete version copies for your records – CYA
  - Use date and draft numbering in file name
- Test Formatting
  - Run test export before committing to a full edit

Signing

Paper Signing
Pros:
- Ink and paper usage – Help the office supply industry
- Slower – better billing
- More Storage options – banker box and/or scan to drive
- Practice signatures
- Easier to forge and alter
Paper Signing

Tips:
- Initial lines in footer on Every page
- Require scans of All pages of originals
  - Paper pages can be swapped / altered
  - Keep a PDF of the entire signed document

Electronic Signing

Pros:
- Save paper and ink
- Faster signing and transmitting
- Electronic storage is simple, cheap, searchable
- More dimensions of authentication:
  - Meta date, IP addresses, signer email, time of signing, third party record
  - Forgery and fraud easier to detect and prove
Electronic Signing

- **Cons:**
  - Paid service
  - Opposing counsel must email client directly
  - PDF may still be editable
  - Emailed link to document may not be secure

**Tips:**
- Get opposing counsel’s permission to send signing invitation to other party
- Flatten and distribute signed PDF
- Kill link to confidential documents
Conclusion – The Golden Age

› Contracts: Codify intent of the parties

› Truth more accessible
  ◦ More writings – emails and texts
  ◦ Better records – communications and timing

Aaron Cronan
Cronan Law LLC
www.cronanlawfirm.com
aaron@cronanlawfirm.com
503–482–9210
CHAPTER 96—ELECTRONIC SIGNATURES IN
GLOBAL AND NATIONAL COMMERCE

SUBCHAPTER I—ELECTRONIC RECORDS AND
SIGNATURES IN COMMERCE

Sec.
7001. General rule of validity.
7002. Exemption to preemption.
7003. Specific exceptions.
7004. Applicability to Federal and State govern-
ments.
7005. Studies.
7006. Definitions.

SUBCHAPTER II—TRANSFERABLE RECORDS

7021. Transferable records.

SUBCHAPTER III—PROMOTION OF
INTERNATIONAL ELECTRONIC COMMERCE

7031. Principles governing the use of electronic sig-
natures in international transactions.

§ 7001. General rule of validity

(a) In general

Notwithstanding any statute, regulation, or other rule of law (other than this subchapter
and subchapter II of this chapter), with respect to any transaction in or affecting interstate or
foreign commerce—

(1) a signature, contract, or other record re-
lated to such transaction may not be denied
legal effect, validity, or enforceability solely
because it is in electronic form; and

(2) a contract relating to such transaction
may not be denied legal effect, validity, or en-
forceability solely because an electronic sig-
nature or electronic record was used in its for-
mation.
(b) Preservation of rights and obligations

This subchapter does not—

(1) limit, alter, or otherwise affect any requirement imposed by a statute, regulation, or rule of law relating to the rights and obligations of persons under such statute, regulation, or rule of law other than a requirement that contracts or other records be written, signed, or in nonelectronic form; or

(2) require any person to agree to use or accept electronic records or electronic signatures, other than a governmental agency with respect to a record other than a contract to which it is a party.

c) Consumer disclosures

(1) Consent to electronic records

Notwithstanding subsection (a) of this section, if a statute, regulation, or other rule of law requires that information relating to a transaction or transactions in or affecting interstate or foreign commerce be provided or made available to a consumer in writing, the use of an electronic record to provide or make available (whichever is required) such information satisfies the requirement that such information be in writing if—

(A) the consumer has affirmatively consented to such use and has not withdrawn such consent;

(B) the consumer, prior to consenting, is provided with a clear and conspicuous statement—

(i) informing the consumer of (I) any right or option of the consumer to have the record provided or made available on paper or in nonelectronic form, and (II) the right of the consumer to withdraw the consent to have the record provided or made available in an electronic form and of any conditions, consequences (which may include termination of the parties’ relationship), or fees in the event of such withdrawal;

(ii) informing the consumer of whether the consent applies (I) only to the particular transaction which gave rise to the obligation to provide the record, or (II) to identified categories of records that may be provided or made available during the course of the parties’ relationship;

(iii) describing the procedures the consumer must use to withdraw consent as provided in clause (i) and to update information needed to contact the consumer electronically; and

(iv) informing the consumer (I) how, after the consent, the consumer may, upon request, obtain a paper copy of an electronic record, and (II) whether any fee will be charged for such copy;

(C) the consumer—

(i) prior to consenting, is provided with a statement of the hardware and software requirements for access to and retention of the electronic records; and

(ii) consents electronically, or confirms his or her consent electronically, in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent; and

(D) after the consent of a consumer in accordance with subparagraph (A), if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a subsequent electronic record that was the subject of the consent, the person providing the electronic record—

(i) provides the consumer with a statement of (I) the revised hardware and software requirements for access to and retention of the electronic records, and (II) the right to withdraw consent without the imposition of any fees for such withdrawal and without the imposition of any condition or consequence that was not disclosed under subparagraph (B)(i); and

(ii) again complies with subparagraph (C).

(2) Other rights

(A) Preservation of consumer protections

Nothing in this subchapter affects the content or timing of any disclosure or other record required to be provided or made available to any consumer under any statute, regulation, or other rule of law.

(B) Verification or acknowledgment

If a law that was enacted prior to this chapter expressly requires a record to be provided or made available by a specified method that requires verification or acknowledgment of receipt, the record may be provided or made available electronically only if the method used provides verification or acknowledgment of receipt (whichever is required).

(3) Effect of failure to obtain electronic consent or confirmation of consent

The legal effectiveness, validity, or enforceability of any contract executed by a consumer shall not be denied solely because of the failure to obtain electronic consent or confirmation of consent by that consumer in accordance with paragraph (1)(C)(i).

(4) Prospective effect

Withdrawal of consent by a consumer shall not affect the legal effectiveness, validity, or enforceability of electronic records provided or made available to that consumer in accordance with paragraph (1) prior to implementation of the consumer’s withdrawal of consent. A consumer’s withdrawal of consent shall be effective within a reasonable period of time after receipt of the withdrawal by the provider of the record. Failure to comply with paragraph (1)(D) may, at the election of the consumer, be treated as a withdrawal of consent for purposes of this paragraph.

(5) Prior consent

This subsection does not apply to any records that are provided or made available to a consumer who has consented prior to the effective date of this subchapter to receive such
records in electronic form as permitted by any statute, regulation, or other rule of law.

(6) Oral communications

An oral communication or a recording of an oral communication shall not qualify as an electronic record for purposes of this subsection except as otherwise provided under applicable law.

(d) Retention of contracts and records

(1) Accuracy and accessibility

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

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

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

(2) Exception

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

(3) Originals

If a statute, regulation, or other rule of law requires a contract or other record relating to a transaction in or affecting interstate or foreign commerce to be provided, available, or retained in its original form, or provides consequences if the contract or other record is not provided, available, or retained in its original form, that statute, regulation, or rule of law is satisfied if the electronic record that complies with paragraph (1).

(4) Checks

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

(e) Accuracy and ability to retain contracts and other records

Notwithstanding subsection (a) of this section, if a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be in writing, the legal effect, validity, or enforceability of an electronic record of such contract or other record may be denied if such electronic record is not in a form that is capable of being retained and accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record.

(f) Proximity

Nothing in this subchapter affects the proximity required by any statute, regulation, or other rule of law with respect to any warning, notice, disclosure, or other record required to be posted, displayed, or publicly affixed.

(g) Notarization and acknowledgment

If a statute, regulation, or other rule of law requires a signature or record relating to a transaction in or affecting interstate or foreign commerce to be notarized, acknowledged, verified, or made under oath, that requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable statute, regulation, or rule of law, is attached to or logically associated with the signature or record.

(h) Electronic agents

A contract or other record relating to a transaction in or affecting interstate or foreign commerce may not be denied legal effect, validity, or enforceability solely because its formation, creation, or delivery involved the action of one or more electronic agents so long as the action of any such electronic agent is legally attributable to the person to be bound.

(i) Insurance

It is the specific intent of the Congress that this subchapter and subchapter II of this chapter apply to the business of insurance.

(j) Insurance agents and brokers

An insurance agent or broker acting under the direction of a party that enters into a contract by means of an electronic record or electronic signature may not be held liable for any deficiency in the electronic procedures agreed to by the parties under that contract if—

(1) the agent or broker has not engaged in negligent, reckless, or intentional tortious conduct;

(2) the agent or broker was not involved in the development or establishment of such electronic procedures; and

(3) the agent or broker did not deviate from such procedures.
“(B) Delayed effect for pending rulemakings.—If on March 1, 2001, a Federal regulatory agency or State regulatory agency has announced, proposed, or initiated, but not completed, a rulemaking proceeding to prescribe a regulation under section 104(b)(3) [15 U.S.C. 7004(b)(3)] with respect to a requirement described in subparagraph (A), this title shall be effective on June 1, 2001, with respect to such requirement.

“(2) Certain guaranteed and insured loans.—With regard to any transaction involving a loan guarantee or loan guarantee commitment (as those terms are defined in section 502 of the Federal Credit Reform Act of 1990 [2 U.S.C. 661a]), or involving a program listed in the Federal Credit Supplement, Budget of the United States, FY 2001, this title applies only to such transactions entered into, and to any loan or mortgage made, insured, or guaranteed by the United States Government thereunder, on and after one year after the date of enactment of this Act [June 30, 2000].

“(3) Student loans.—With respect to any records that are provided or made available to a consumer pursuant to an application for a loan, or a loan made, pursuant to title IV of the Higher Education Act of 1965 [20 U.S.C. 1070 et seq., 42 U.S.C. 2751 et seq.], section 101(c) of this Act [15 U.S.C. 7001(c)] shall not apply until the earlier of—

“(A) such time as the Secretary of Education publishes revised promissory notes under section 432(m) of the Higher Education Act of 1965 [20 U.S.C. 1082(m)]; or

“(B) one year after the date of enactment of this Act [June 30, 2000]."

**Short Title**

Pub. L. 106–229, §1, June 30, 2000, 114 Stat. 464, provided that: “This Act [enacting this chapter and amending provisions set out as a note under section 231 of Title 47, Telegraphs, Telephones, and Radiotelegraphs] may be cited as the ‘Electronic Signatures in Global and National Commerce Act.’”
UNIFORM ELECTRONIC TRANSACTIONS ACT (1999)

Drafted by the

NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS

and by it

APPROVED AND RECOMMENDED FOR ENACTMENT
IN ALL THE STATES

at its

ANNUAL CONFERENCE
MEETING IN ITS ONE-HUNDRED-AND-EIGHTH YEAR
IN DENVER, COLORADO
JULY 23 – 30, 1999

WITH PREFATORY NOTE AND COMMENTS

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

Approved by the American Bar Association
Dallas, Texas, February 14, 2000

1/20/00
UNIFORM ELECTRONIC TRANSACTIONS ACT (1999)

The Committee that acted for the National Conference of Commissioners on Uniform State Laws in preparing the Uniform Electronic Transactions Act (1999) was as follows:

PATRICIA BRUMFIELD FRY, University of North Dakota, School of Law, P.O. Box 9003, Grand Forks, ND 58201, Chair
STEPHEN Y. CHOW, 30th Floor, One Beacon St., Boston, MA 02108
KENNETH W. ELLIOTT, City Place Building, 22nd Floor, 204 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 the Attorney General, P.O. Box 201401, 215 N. Sanders, Helena, MT 59620
PAMELA MEADE SARGENT, P.O. Box 846, Abingdon, VA 24212
D. BENJAMIN BEARD, University of Idaho, College of Law, 6th and Rayburn, Moscow, ID 83844-2321, Reporter

EX OFFICIO

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

AMERICAN BAR ASSOCIATION ADVISORS

C. ROBERT BEATTIE, Plaza VII, 45 S. 7th Street, Suite 3400, Minneapolis, MN 55402-1609, Business Law Section
AMELIA H. BOSS, Temple University, School of Law, 1719 N. Broad Street, Philadelphia, PA 19122, Advisor
THOMAS J. SMEDINGHOFF, 130 E. Randolph Drive, Suite 3500, Chicago, IL 60601, Science and Technology Section

EXECUTIVE DIRECTOR

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

Copies of this Act may be obtained from:

NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS
211 E. Ontario Street, Suite 1300
Chicago, Illinois 60611
# UNIFORM ELECTRONIC TRANSACTIONS ACT (1999)

## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SHORT TITLE</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>DEFINITIONS</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>SCOPE</td>
<td>13</td>
</tr>
<tr>
<td>4</td>
<td>PROSPECTIVE APPLICATION</td>
<td>20</td>
</tr>
<tr>
<td>5</td>
<td>USE OF ELECTRONIC RECORDS AND ELECTRONIC SIGNATURES; VARIATION BY AGREEMENT</td>
<td>20</td>
</tr>
<tr>
<td>6</td>
<td>CONSTRUCTION AND APPLICATION</td>
<td>24</td>
</tr>
<tr>
<td>7</td>
<td>LEGAL RECOGNITION OF ELECTRONIC RECORDS, ELECTRONIC SIGNATURES, AND ELECTRONIC CONTRACTS</td>
<td>26</td>
</tr>
<tr>
<td>8</td>
<td>PROVISION OF INFORMATION IN WRITING; PRESENTATION OF RECORDS</td>
<td>28</td>
</tr>
<tr>
<td>9</td>
<td>ATTRIBUTION AND EFFECT OF ELECTRONIC RECORD AND ELECTRONIC SIGNATURE</td>
<td>31</td>
</tr>
<tr>
<td>10</td>
<td>EFFECT OF CHANGE OR ERROR</td>
<td>33</td>
</tr>
<tr>
<td>11</td>
<td>NOTARIZATION AND ACKNOWLEDGMENT</td>
<td>37</td>
</tr>
<tr>
<td>12</td>
<td>RETENTION OF ELECTRONIC RECORDS; ORIGINALS</td>
<td>38</td>
</tr>
<tr>
<td>13</td>
<td>ADMISSION IN EVIDENCE</td>
<td>42</td>
</tr>
<tr>
<td>14</td>
<td>AUTOMATED TRANSACTION</td>
<td>42</td>
</tr>
<tr>
<td>15</td>
<td>TIME AND PLACE OF SENDING AND RECEIPT</td>
<td>44</td>
</tr>
<tr>
<td>16</td>
<td>TRANSFERABLE RECORDS</td>
<td>48</td>
</tr>
<tr>
<td>17</td>
<td>CREATION AND RETENTION OF ELECTRONIC RECORDS AND CONVERSION OF WRITTEN RECORDS BY GOVERNMENTAL AGENCIES</td>
<td>56</td>
</tr>
<tr>
<td>18</td>
<td>ACCEPTANCE AND DISTRIBUTION OF ELECTRONIC RECORDS BY GOVERNMENTAL AGENCIES</td>
<td>56</td>
</tr>
<tr>
<td>19</td>
<td>INTEROPERABILITY</td>
<td>58</td>
</tr>
<tr>
<td>20</td>
<td>SEVERABILITY CLAUSE</td>
<td>61</td>
</tr>
<tr>
<td>21</td>
<td>EFFECTIVE DATE</td>
<td>61</td>
</tr>
</tbody>
</table>
UNIFORM ELECTRONIC TRANSACTIONS ACT (1999)

PREFATORY NOTE

With the advent of electronic means of communication and information transfer, business models and methods for doing business have evolved to take advantage of the speed, efficiencies, and cost benefits of electronic technologies. These developments have occurred in the face of existing legal barriers to the legal efficacy of records and documents which exist solely in electronic media. Whether the legal requirement that information or an agreement or contract must be contained or set forth in a pen and paper writing derives from a statute of frauds affecting the enforceability of an agreement, or from a record retention statute that calls for keeping the paper record of a transaction, such legal requirements raise real barriers to the effective use of electronic media.

One striking example of electronic barriers involves so called check retention statutes in every State. A study conducted by the Federal Reserve Bank of Boston identified more than 2500 different state laws which require the retention of canceled checks by the issuers of those checks. These requirements not only impose burdens on the issuers, but also effectively restrain the ability of banks handling the checks to automate the process. Although check truncation is validated under the Uniform Commercial Code, if the bank’s customer must store the canceled paper check, the bank will not be able to deal with the item through electronic transmission of the information. By establishing the equivalence of an electronic record of the information, the Uniform Electronic Transactions Act (UETA) removes these barriers without affecting the underlying legal rules and requirements.

It is important to understand that the purpose of the UETA is to remove barriers to electronic commerce by validating and effectuating electronic records and signatures. It is NOT a general contracting statute – the substantive rules of contracts remain unaffected by UETA. Nor is it a digital signature statute. To the extent that a State has a Digital Signature Law, the UETA is designed to support and compliment that statute.

A. Scope of the Act and Procedural Approach. The scope of this Act provides coverage which sets forth a clear framework for covered transactions, and also avoids unwarranted surprises for unsophisticated parties dealing in this relatively new media. The clarity and certainty of the scope of the Act have been obtained while still providing a solid legal framework that allows for the continued development of innovative technology to facilitate electronic transactions.
With regard to the general scope of the Act, the Act’s coverage is inherently limited by the definition of “transaction.” The Act does not apply to all writings and signatures, but only to electronic records and signatures relating to a transaction, defined as those interactions between people relating to business, commercial and governmental affairs. In general, there are few writing or signature requirements imposed by law on many of the “standard” transactions that had been considered for exclusion. A good example relates to trusts, where the general rule on creation of a trust imposes no formal writing requirement. Further, the writing requirements in other contexts derived from governmental filing issues. For example, real estate transactions were considered potentially troublesome because of the need to file a deed or other instrument for protection against third parties. Since the efficacy of a real estate purchase contract, or even a deed, between the parties is not affected by any sort of filing, the question was raised why these transactions should not be validated by this Act if done via an electronic medium. No sound reason was found. Filing requirements fall within Sections 17-19 on governmental records. An exclusion of all real estate transactions would be particularly unwarranted in the event that a State chose to convert to an electronic recording system, as many have for Article 9 financing statement filings under the Uniform Commercial Code.

The exclusion of specific Articles of the Uniform Commercial Code reflects the recognition that, particularly in the case of Articles 5, 8 and revised Article 9, electronic transactions were addressed in the specific contexts of those revision processes. In the context of Articles 2 and 2A the UETA provides the vehicle for assuring that such transactions may be accomplished and effected via an electronic medium. At such time as Articles 2 and 2A are revised the extent of coverage in those Articles/Acts may make application of this Act as a gap-filling law desirable. Similar considerations apply to the recently promulgated Uniform Computer Information Transactions Act (“UCITA”).

The need for certainty as to the scope and applicability of this Act is critical, and makes any sort of a broad, general exception based on notions of inconsistency with existing writing and signature requirements unwise at best. The uncertainty inherent in leaving the applicability of the Act to judicial construction of this Act with other laws is unacceptable if electronic transactions are to be facilitated.

Finally, recognition that the paradigm for the Act involves two willing parties conducting a transaction electronically, makes it necessary to expressly provide that some form of acquiescence or intent on the part of a person to conduct transactions electronically is necessary before the Act can be invoked. Accordingly, Section 5 specifically provides that the Act only applies between parties that have agreed to conduct transactions electronically. In this context, the construction of the term agreement must be broad in order to assure that the Act
applies whenever the circumstances show the parties intention to transact electronically, regardless of whether the intent rises to the level of a formal agreement.

**B. Procedural Approach.** Another fundamental premise of the Act is that it be minimalist and procedural. The general efficacy of existing law in an electronic context, so long as biases and barriers to the medium are removed, validates this approach. The Act defers to existing substantive law. Specific areas of deference to other law in this Act include: (1) the meaning and effect of “sign” under existing law, (2) the method and manner of displaying, transmitting and formatting information in Section 8, (3) rules of attribution in Section 9, and (4) the law of mistake in Section 10.

The Act’s treatment of records and signatures demonstrates best the minimalist approach that has been adopted. Whether a record is attributed to a person is left to law outside this Act. Whether an electronic signature has any effect is left to the surrounding circumstances and other law. These provisions are salutary directives to assure that records and signatures will be treated in the same manner, under currently existing law, as written records and manual signatures.

The deference of the Act to other substantive law does not negate the necessity of setting forth rules and standards for using electronic media. The Act expressly validates electronic records, signatures and contracts. It provides for the use of electronic records and information for retention purposes, providing certainty in an area with great potential in cost savings and efficiency. The Act makes clear that the actions of machines (“electronic agents”) programmed and used by people will bind the user of the machine, regardless of whether human review of a particular transaction has occurred. It specifies the standards for sending and receipt of electronic records, and it allows for innovation in financial services through the implementation of transferable records. In these ways the Act permits electronic transactions to be accomplished with certainty under existing substantive rules of law.
UNIFORM ELECTRONIC TRANSACTIONS ACT (1999)

SECTION 1. SHORT TITLE. This [Act] may be cited as the Uniform Electronic Transactions Act.

SECTION 2. DEFINITIONS. In this [Act]:

(1) “Agreement” means the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations, and procedures given the effect of agreements under laws otherwise applicable to a particular transaction.

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

(3) “Computer program” means a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result.

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

(5) “Electronic” means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
(6) “Electronic agent” means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual.

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

(8) “Electronic signature” means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

(9) “Governmental agency” means an executive, legislative, or judicial agency, department, board, commission, authority, institution, or instrumentality of the federal government or of a State or of a county, municipality, or other political subdivision of a State.

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

(11) “Information processing system” means an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information.

(12) “Person” means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or any other legal or commercial entity.
(13) “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.

(14) “Security procedure” means a procedure employed 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 information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.

(15) “State” means a State of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any territory or insular possession subject to the jurisdiction of the United States. The term includes an Indian tribe or band, or Alaskan native village, which is recognized by federal law or formally acknowledged by a State.

(16) “Transaction” means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

Sources: UNICTRAL Model Law on Electronic Commerce; Uniform Commercial Code; Uniform Computer Information Transactions Act; Restatement 2d Contracts.

Comment

1. “Agreement.”

Whether the parties have reached an agreement is determined by their express language and all surrounding circumstances. The Restatement 2d Contracts § 3 provides that, “An agreement is a manifestation of mutual assent on the part of
two or more persons.” See also Restatement 2d Contracts, Section 2, Comment b. 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. Although the definition of agreement in this Act does not make specific reference to usage of trade and other party conduct, this definition is not intended to affect the construction of the parties’ agreement under the substantive law applicable to a particular transaction. Where that law takes account of usage and conduct in informing the terms of the parties’ agreement, the usage or conduct would be relevant as “other circumstances” included in the definition under this Act.

Where the law applicable to a given transaction provides that system rules and the like constitute part of the agreement of the parties, such rules will have the same effect in determining the parties agreement under this Act. For example, UCC Article 4 (Section 4-103(b)) provides that Federal Reserve regulations and operating circulars and clearinghouse rules have the effect of agreements. Such agreements by law properly would be included in the definition of agreement in this Act.

The parties’ agreement is relevant in determining whether the provisions of this Act have been varied by agreement. In addition, the parties’ agreement may establish the parameters of the parties’ use of electronic records and signatures, security procedures and similar aspects of the transaction. See Model Trading Partner Agreement, 45 Business Lawyer Supp. Issue (June 1990). See Section 5(b) and Comments thereto.

2. “Automated Transaction.”

An automated transaction is a transaction performed or conducted by electronic means in which machines are used without human intervention to form contracts and perform obligations under existing contracts. Such broad coverage is necessary 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 14 provides specific rules to assure that where one or both parties do not review the electronic records, the resulting agreement will be effective.

The critical element in this definition is the lack of a human actor on one or both sides of a transaction. For example, if one orders books from Bookseller.com through Bookseller’s website, the transaction would be an automated transaction because Bookseller took and confirmed the order via its machine. Similarly, if
Automaker and supplier do business through Electronic Data Interchange, Automaker’s computer, upon receiving information within certain pre-programmed parameters, will send an electronic order to supplier’s computer. If Supplier’s computer confirms the order and processes the shipment because the order falls within pre-programmed parameters in Supplier’s computer, this would be a fully automated transaction. If, instead, the Supplier relies on a human employee to review, accept, and process the Buyer’s order, then only the Automaker’s side of the transaction would be automated. In either case, the entire transaction falls within this definition.

3. “Computer program.” This definition refers to the functional and operating aspects of an electronic, digital system. It relates to operating instructions used in an electronic system such as an electronic agent. (See definition of “Electronic Agent.”)

4. “Electronic.” The basic nature of most current technologies and the need for a recognized, single term warrants the use of “electronic” as the defined term. The definition is intended to assure that the Act will be applied broadly as new technologies develop. The term must be construed broadly in light of developing technologies in order to fulfill the purpose of this Act to validate commercial transactions regardless of the medium used by the parties. Current legal requirements for “writings” can be satisfied by almost any tangible media, whether paper, other fibers, or even stone. The purpose and applicability of this Act covers intangible media which are technologically capable of storing, transmitting and reproducing information in human perceivable form, but which lack the tangible aspect of paper, papyrus or stone.

While not all technologies listed are technically “electronic” in nature (e.g., optical fiber technology), the term “electronic” is the most descriptive term available to describe the majority of current technologies. For example, the development of biological and chemical processes for communication and storage of data, while not specifically mentioned in the definition, are included within the technical definition because such processes operate on electromagnetic impulses. However, whether a particular technology may be characterized as technically “electronic,” i.e., operates on electromagnetic impulses, should not be determinative of whether records and signatures created, used and stored by means of a particular technology are covered by this Act. This Act is intended to apply to all records and signatures created, used and stored by any medium which permits the information to be retrieved in perceivable form.

5. “Electronic agent.” This definition establishes that an electronic agent is a machine. As the term “electronic agent” has come to be recognized, it is
limited to a tool function. The effect on the party using the agent is addressed in the operative provisions of the Act (e.g., Section 14)

An electronic agent, such as a computer program or other automated means employed by a person, is a tool of that person. As a general rule, the employer of a tool is responsible for the results obtained by 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.

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). If such developments occur, courts may construe the definition of electronic agent accordingly, in order to recognize such new capabilities.

The examples involving Bookseller.com and Automaker in the Comment to the definition of Automated Transaction are equally applicable here. Bookseller acts through an electronic agent in processing an order for books. Automaker and the supplier each act through electronic agents in facilitating and effectuating the just-in-time inventory process through EDI.

6. “Electronic record.” An electronic record is a subset of the broader defined term “record.” It is any record created, used or stored in a medium other than paper (see definition of electronic). The defined term is also used in this Act as a limiting definition in those provisions in which it is used.

Information processing systems, computer equipment and programs, electronic data interchange, electronic mail, voice mail, facsimile, telex, teletyping, scanning, and similar technologies all qualify as electronic under this Act. Accordingly information stored on a computer hard drive or floppy disc, facsimiles, voice mail messages, messages on a telephone answering machine, audio and video tape recordings, among other records, all would be electronic records under this Act.
7. “Electronic signature.”

The idea of a signature is broad and not specifically defined. Whether any particular record is “signed” is a question of fact. Proof of that fact must be made under other applicable law. This Act simply assures that the signature may be accomplished through electronic means. No specific technology need be used in order to create a valid signature. One’s voice on an answering machine may suffice if the requisite intention is present. Similarly, including one’s name as part of an electronic mail communication also may suffice, as may the firm name on a facsimile. It also may be shown that the requisite intent was not present and accordingly the symbol, sound or process did not amount to a signature. One may use a digital signature with the requisite intention, or one may use the private key solely as an access device with no intention to sign, or otherwise accomplish a legally binding act. In any case the critical element is the intention to execute or adopt the sound or symbol or process for the purpose of signing the related record.

The definition requires that the signer execute or adopt the sound, symbol, or process with the intent to sign the record. The act of applying a sound, symbol or process to an electronic record could have differing meanings and effects. The consequence of the act and the effect of the act as a signature are determined under other applicable law. However, the essential attribute of a signature involves applying a sound, symbol or process with an intent to do a legally significant act. It is that intention that is understood in the law as a part of the word “sign”, without the need for a definition.

This Act establishes, to the greatest extent possible, the equivalency of electronic signatures and manual signatures. Therefore the term “signature” has been used to connote and convey that equivalency. The purpose is to overcome unwarranted biases against electronic methods of signing and authenticating records. The term “authentication,” used in other laws, often has a narrower meaning and purpose than an electronic signature as used in this Act. However, an authentication under any of those other laws constitutes an electronic signature under this Act.

The precise effect of an electronic signature will be determined based on the surrounding circumstances under Section 9(b).

This definition includes as an electronic signature the standard webpage click through process. For example, when a person orders goods or services through a vendor’s website, the person will be required to provide information as part of a process which will result in receipt of the goods or services. When the customer ultimately gets to the last step and clicks “I agree,” the person has adopted the process and has done so with the intent to associate the person with the record.
of that process. The actual effect of the electronic signature will be determined from all the surrounding circumstances, however, the person adopted a process which the circumstances indicate s/he intended to have the effect of getting the goods/services and being bound to pay for them. The adoption of the process carried the intent to do a legally significant act, the hallmark of a signature.

Another important aspect of this definition lies in the necessity that the electronic signature be linked or logically associated with the record. 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, e.g., an allonge firmly attached to a promissory note, or the classic signature at the end of a long contract. 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 connected with, the electronic record being signed. This linkage is consistent with the regulations promulgated by the Food and Drug Administration. 21 CFR Part 11 (March 20, 1997).

A digital signature using public key encryption technology would qualify as an electronic signature, as would the mere inclusion of one’s name as a part of an e-mail message – so long as in each case the signer executed or adopted the symbol with the intent to sign.

8. “Governmental agency.” This definition is important in the context of optional Sections 17-19.

9. “Information processing system.” This definition is consistent with the UNCITRAL Model Law on Electronic Commerce. The term includes computers and other information systems. It is principally used in Section 15 in connection with the sending and receiving of information. In that context, the key aspect is that the information enter a system from which a person can access it.

10. “Record.” This is a standard definition designed to embrace all means of communicating or storing information except human memory. It includes any method for storing or communicating information, including “writings.” A record need not be indestructible or permanent, but the term does not include oral or other communications which are not stored or preserved by some means. Information that has not been retained other than through human memory does not qualify as a record. As in the case of the terms “writing” or “written,” the term “record” does not establish the purposes, permitted uses or legal effect which a record may have under any particular provision of substantive law. ABA Report on Use of the Term “Record,” October 1, 1996.
11. “Security procedure.”

A security procedure may be applied to verify an electronic signature, verify the identity of the sender, or assure 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.

The definition in this Act is broad and is used to illustrate one way of establishing attribution or content integrity of an electronic record or signature. The use of a security procedure is not accorded operative legal effect, through the use of presumptions or otherwise, by this Act. In this Act, the use of security procedures is simply one method for proving the source or content of an electronic record or signature.

A security procedure may be technologically very sophisticated, such as an asymmetric cryptographic system. At the other extreme the security procedure may be as simple as a telephone call to confirm the identity of the sender through another channel of communication. It may include the use of a mother’s maiden name or a personal identification number (PIN). Each of these examples is a method for confirming the identity of a person or accuracy of a message.

12. “Transaction.” The definition has been limited to actions between people taken in the context of business, commercial or governmental activities. The term includes all interactions between people for business, commercial, including specifically consumer, or governmental purposes. However, the term does not include unilateral or non-transactional actions. As such it provides a structural limitation on the scope of the Act as stated in the next section.

It is essential that the term commerce and business be understood and construed broadly to include commercial and business transactions involving individuals who may qualify as “consumers” under other applicable law. If Alice and Bob agree to the sale of Alice’s car to Bob for $2000 using an internet auction site, that transaction is fully covered by this Act. Even if Alice and Bob each qualify as typical “consumers” under other applicable law, their interaction is a transaction in commerce. Accordingly their actions would be related to commercial affairs, and fully qualify as a transaction governed by this Act.

Other transaction types include:
1. A single purchase by an individual from a retail merchant, which may be accomplished by an order from a printed catalog sent by facsimile, or by exchange of electronic mail.

2. Recurring orders on a weekly or monthly basis between large companies which have entered into a master trading partner agreement to govern the methods and manner of their transaction parameters.

3. A purchase by an individual from an online internet retail vendor. Such an arrangement may develop into an ongoing series of individual purchases, with security procedures and the like, as a part of doing ongoing business.

4. The closing of a business purchase transaction via facsimile transmission of documents or even electronic mail. In such a transaction, all parties may participate through electronic conferencing technologies. At the appointed time all electronic records are executed electronically and transmitted to the other party. In such a case, the electronic records and electronic signatures are validated under this Act, obviating the need for “in person” closings.

A transaction must include interaction between two or more persons. Consequently, to the extent that the execution of a will, trust, or a health care power of attorney or similar health care designation does not involve another person and is a unilateral act, it would not be covered by this Act because not occurring as a part of a transaction as defined in this Act. However, this Act does apply to all electronic records and signatures related to a transaction, and so does cover, for example, internal auditing and accounting records related to a transaction.

SECTION 3. SCOPE.

(a) Except as otherwise provided in subsection (b), this [Act] applies to electronic records and electronic signatures relating to a transaction.

(b) This [Act] does not apply to a transaction to the extent it is governed by:

(1) a law governing the creation and execution of wills, codicils, or testamentary trusts;

(2) [The Uniform Commercial Code other than Sections 1-107 and 1-206, Article 2, and Article 2A];
(3) [the Uniform Computer Information Transactions Act]; and

(4) [other laws, if any, identified by State].

(c) This [Act] applies to an electronic record or electronic signature otherwise excluded from the application of this [Act] under subsection (b) to the extent it is governed by a law other than those specified in subsection (b).

(d) A transaction subject to this [Act] is also subject to other applicable substantive law.

See Legislative Note below – Following Comments.

Comment

1. The scope of this Act is inherently limited by the fact that it only applies to transactions related to business, commercial (including consumer) and governmental matters. Consequently, transactions with no relation to business, commercial or governmental transactions would not be subject to this Act. Unilaterally generated electronic records and signatures which are not part of a transaction also are not covered by this Act. See Section 2, Comment 12.

2. This Act affects the medium in which information, records and signatures may be presented and retained under current legal requirements. While this Act covers all electronic records and signatures which are used in a business, commercial (including consumer) or governmental transaction, the operative provisions of the Act relate to requirements for writings and signatures under other laws. Accordingly, the exclusions in subsection (b) focus on those legal rules imposing certain writing and signature requirements which will not be affected by this Act.

3. The exclusions listed in subsection (b) provide clarity and certainty regarding the laws which are and are not affected by this Act. This section provides that transactions subject to specific laws are unaffected by this Act and leaves the balance subject to this Act.

4. Paragraph (1) excludes wills, codicils and testamentary trusts. This exclusion is largely salutary given the unilateral context in which such records are generally created and the unlikely use of such records in a transaction as defined in this Act (i.e., actions taken by two or more persons in the context of business, commercial or governmental affairs). Paragraph (2) excludes all of the Uniform
Commercial Code other than UCC Sections 1-107 and 1-206, and Articles 2 and 2A. This Act does not apply to the excluded UCC articles, whether in “current” or “revised” form. The Act does apply to UCC Articles 2 and 2A and to UCC Sections 1-107 and 1-206.

5. Articles 3, 4 and 4A of the UCC impact payment systems and have specifically been removed from the coverage of this Act. The check collection and electronic fund transfer systems governed by Articles 3, 4 and 4A involve systems and relationships involving numerous parties beyond the parties to the underlying contract. The impact of validating electronic media in such systems involves considerations beyond the scope of this Act. Articles 5, 8 and 9 have been excluded because the revision process relating to those Articles included significant consideration of electronic practices. Paragraph 4 provides for exclusion from this Act of the Uniform Computer Information Transactions Act (UCITA) because the drafting process of that Act also included significant consideration of electronic contracting provisions.

6. The very limited application of this Act to Transferable Records in Section 16 does not affect payment systems, and the section is designed to apply to a transaction only through express agreement of the parties. The exclusion of Articles 3 and 4 will not affect the Act’s coverage of Transferable Records. Section 16 is designed to allow for the development of systems which will provide “control” as defined in Section 16. Such control is necessary as a substitute for the idea of possession which undergirds negotiable instrument law. The technology has yet to be developed which will allow for the possession of a unique electronic token embodying the rights associated with a negotiable promissory note. Section 16’s concept of control is intended as a substitute for possession.

The provisions in Section 16 operate as free standing rules, establishing the rights of parties using Transferable Records under this Act. The references in Section 16 to UCC Sections 3-302, 7-501, and 9-308 (R9-330(d)) are designed to incorporate the substance of those provisions into this Act for the limited purposes noted in Section 16(c). Accordingly, an electronic record which is also a Transferable Record, would not be used for purposes of a transaction governed by Articles 3, 4, or 9, but would be an electronic record used for purposes of a transaction governed by Section 16. However, it is important to remember that those UCC Articles will still apply to the transferable record in their own right. Accordingly any other substantive requirements, e.g., method and manner of perfection under Article 9, must be complied with under those other laws. See Comments to Section 16.

7. This Act does apply, in toto, to transactions under unrevised Articles 2 and 2A. There is every reason to validate electronic contracting in these situations.
Sale and lease transactions do not implicate broad systems beyond the parties to the underlying transaction, such as are present in check collection and electronic funds transfers. Further sales and leases generally do not have as far reaching effect on the rights of third parties beyond the contracting parties, such as exists in the secured transactions system. Finally, it is in the area of sales, licenses and leases that electronic commerce is occurring to its greatest extent today. To exclude these transactions would largely gut the purpose of this Act.

In the event that Articles 2 and 2A are revised and adopted in the future, UETA will only apply to the extent provided in those Acts.

8. An electronic record/signature may be used for purposes of more than one legal requirement, or may be covered by more than one law. Consequently, it is important to make clear, despite any apparent redundancy, in subsection (c) that an electronic record used for purposes of a law which is not affected by this Act under subsection (b) may nonetheless be used and validated for purposes of other laws not excluded by subsection (b). For example, this Act does not apply to an electronic record of a check when used for purposes of a transaction governed by Article 4 of the Uniform Commercial Code, i.e., the Act does not validate so-called electronic checks. However, for purposes of check retention statutes, the same electronic record of the check is covered by this Act, so that retention of an electronic image/record of a check will satisfy such retention statutes, so long as the requirements of Section 12 are fulfilled.

In another context, subsection (c) would operate to allow this Act to apply to what would appear to be an excluded transaction under subsection (b). For example, Article 9 of the Uniform Commercial Code applies generally to any transaction that creates a security interest in personal property. However, Article 9 excludes landlord’s liens. Accordingly, although this Act excludes from its application transactions subject to Article 9, this Act would apply to the creation of a landlord lien if the law otherwise applicable to landlord’s liens did not provide otherwise, because the landlord’s lien transaction is excluded from Article 9.

9. Additional exclusions under subparagraph (b)(4) should be limited to laws which govern electronic records and signatures which may be used in transactions as defined in Section 2(16). Records used unilaterally, or which do not relate to business, commercial (including consumer), or governmental affairs are not governed by this Act in any event, and exclusion of laws relating to such records may create unintended inferences about whether other records and signatures are covered by this Act.

It is also important that additional exclusions, if any, be incorporated under subsection (b)(4). As noted in Comment 8 above, an electronic record used in a
transaction excluded under subsection (b), e.g., a check used to pay one’s taxes, will nonetheless be validated for purposes of other, non-excluded laws under subsection (c), e.g., the check when used as proof of payment. It is critical that additional exclusions, if any, be incorporated into subsection (b) so that the salutary effect of subsection (c) apply to validate those records in other, non-excluded transactions. While a legislature may determine that a particular notice, such as a utility shutoff notice, be provided to a person in writing on paper, it is difficult to see why the utility should not be entitled to use electronic media for storage and evidentiary purposes. \textit{Legislative Note Regarding Possible Additional Exclusions under Section 3(b)(4)}.

The following discussion is derived from the Report dated September 21, 1998 of The Task Force on State Law Exclusions (the “Task Force”) presented to the Drafting Committee. After consideration of the Report, the Drafting Committee determined that exclusions other than those specified in the Act were not warranted. In addition, other inherent limitations on the applicability of the Act (the definition of transaction, the requirement that the parties acquiesce in the use of an electronic format) also militate against additional exclusions. Nonetheless, the Drafting Committee recognized that some legislatures may wish to exclude additional transactions from the Act, and determined that guidance in some major areas would be helpful to those legislatures considering additional areas for exclusion.

Because of the overwhelming number of references in state law to writings and signatures, the following list of possible transactions is not exhaustive. However, they do represent those areas most commonly raised during the course of the drafting process as areas that might be inappropriate for an electronic medium. It is important to keep in mind however, that the Drafting Committee determined that exclusion of these additional areas was not warranted.

1. \textbf{Trusts} (other than testamentary trusts). Trusts can be used for both business and personal purposes. By virtue of the definition of transaction, trusts used outside the area of business and commerce would not be governed by this Act. With respect to business or commercial trusts, the laws governing their formation contain few or no requirements for paper or signatures. Indeed, in most jurisdictions trusts of any kind may be created orally. Consequently, the Drafting Committee believed that the Act should apply to any transaction where the law leaves to the parties the decision of whether to use a writing. Thus, in the absence of legal requirements for writings, there is no sound reason to exclude laws governing trusts from the application of this Act.

2. \textbf{Powers of Attorney}. A power of attorney is simply a formalized type of agency agreement. In general, no formal requirements for paper or execution were found to be applicable to the validity of powers of attorney.
Special health powers of attorney have been established by statute in some States. These powers may have special requirements under state law regarding execution, acknowledgment and possibly notarization. In the normal case such powers will not arise in a transactional context and so would not be covered by this Act. However, even if such a record were to arise in a transactional context, this Act operates simply to remove the barrier to the use of an electronic medium, and preserves other requirements of applicable substantive law, avoiding any necessity to exclude such laws from the operation of this Act. Especially in light of the provisions of Sections 8 and 11, the substantive requirements under such laws will be preserved and may be satisfied in an electronic format.

3. **Real Estate Transactions.** It is important to distinguish between the efficacy of paper documents involving real estate between the parties, as opposed to their effect on third parties. As between the parties it is unnecessary to maintain existing barriers to electronic contracting. There are no unique characteristics to contracts relating to real property as opposed to other business and commercial (including consumer) contracts. Consequently, the decision whether to use an electronic medium for their agreements should be a matter for the parties to determine. Of course, to be effective against third parties state law generally requires filing with a governmental office. Pending adoption of electronic filing systems by States, the need for a piece of paper to file to perfect rights against third parties, will be a consideration for the parties. In the event notarization and acknowledgment are required under other laws, Section 11 provides a means for such actions to be accomplished electronically.

With respect to the requirements of government filing, those are left to the individual States in the decision of whether to adopt and implement electronic filing systems. (See optional Sections 17-19.) However, government recording systems currently require paper deeds including notarized, manual signatures. Although California and Illinois are experimenting with electronic filing systems, until such systems become widespread, the parties likely will choose to use, at the least, a paper deed for filing purposes. Nothing in this Act precludes the parties from selecting the medium best suited to the needs of the particular transaction. Parties may wish to consummate the transaction using electronic media in order to avoid expensive travel. Yet the actual deed may be in paper form to assure compliance with existing recording systems and requirements. The critical point is that nothing in this Act prevents the parties from selecting paper or electronic media for all or part of their transaction.

4. **Consumer Protection Statutes.** Consumer protection provisions in state law often require that information be disclosed or provided to a consumer in writing. Because this Act does apply to such transactions, the question of whether such laws should be specifically excluded was considered. Exclusion of consumer
transactions would eliminate a huge group of commercial transactions which benefit consumers by enabling the efficiency of the electronic medium. Commerce over the internet is driven by consumer demands and concerns and must be included.

At the same time, it is important to recognize the protective effects of many consumer statutes. Consumer statutes often require that information be provided in writing, or may require that the consumer separately sign or initial a particular provision to evidence that the consumer’s attention was brought to the provision. Subsection (1) requires electronic records to be retainable by a person whenever the law requires information to be delivered in writing. The section imposes a significant burden on the sender of information. The sender must assure that the information system of the recipient is compatible with, and capable of retaining the information sent by, the sender’s system. Furthermore, nothing in this Act permits the avoidance of legal requirements of separate signatures or initialing. The Act simply permits the signature or initialing to be done electronically.

Other consumer protection statutes require (expressly or implicitly) that certain information be presented in a certain manner or format. Laws requiring information to be presented in particular fonts, formats or in similar fashion, as well as laws requiring conspicuous displays of information are preserved. Section 8(b)(3) specifically preserves the applicability of such requirements in an electronic environment. In the case of legal requirements that information be presented or appear conspicuous, the determination of what is conspicuous will be left to other law. Section 8 was included to specifically preserve the protective functions of such disclosure statutes, while at the same time allowing the use of electronic media if the substantive requirements of the other laws could be satisfied in the electronic medium.

Formatting and separate signing requirements serve a critical purpose in much consumer protection legislation, to assure that information is not slipped past the unsuspecting consumer. Not only does this Act not disturb those requirements, it preserves those requirements. In addition, other bodies of substantive law continue to operate to allow the courts to police any such bad conduct or overreaching, e.g., unconscionability, fraud, duress, mistake and the like. These bodies of law remain applicable regardless of the medium in which a record appears.

The requirement that both parties agree to conduct a transaction electronically also prevents the imposition of an electronic medium on unwilling parties See Section 5(b). In addition, where the law requires inclusion of specific terms or language, those requirements are preserved broadly by Section 5(e).
Requirements that information be sent to, or received by, someone have been preserved in Section 15. As in the paper world, obligations to send do not impose any duties on the sender to assure receipt, other than reasonable methods of dispatch. In those cases where receipt is required legally, Sections 5, 8, and 15 impose the burden on the sender to assure delivery to the recipient if satisfaction of the legal requirement is to be fulfilled.

The preservation of existing safeguards, together with the ability to opt out of the electronic medium entirely, demonstrate the lack of any need generally to exclude consumer protection laws from the operation of this Act. Legislatures may wish to focus any review on those statutes which provide for post-contract formation and post-breach notices to be in paper. However, any such consideration must also balance the needed protections against the potential burdens which may be imposed. Consumers and others will not be well served by restrictions which preclude the employment of electronic technologies sought and desired by consumers.

SECTION 4. PROSPECTIVE APPLICATION. This [Act] applies to any electronic record or electronic signature created, generated, sent, communicated, received, or stored on or after the effective date of this [Act].

Comment

This section makes clear that the Act only applies to validate electronic records and signatures which arise subsequent to the effective date of the Act. Whether electronic records and electronic signatures arising before the effective date of this Act are valid is left to other law.

SECTION 5. USE OF ELECTRONIC RECORDS AND ELECTRONIC SIGNATURES; VARIATION BY AGREEMENT.

(a) This [Act] does not require a record or signature to be created, generated, sent, communicated, received, stored, or otherwise processed or used by electronic means or in electronic form.
(b) This [Act] applies only to transactions between parties each of which has agreed to conduct transactions by electronic means. Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties’ conduct.

(c) A party that agrees to conduct a transaction by electronic means may refuse to conduct other transactions by electronic means. The right granted by this subsection may not be waived by agreement.

(d) Except as otherwise provided in this [Act], the effect of any of its provisions may be varied by agreement. 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.

(e) Whether an electronic record or electronic signature has legal consequences is determined by this [Act] and other applicable law.

Comment

This section limits the applicability of this Act to transactions which parties have agreed to conduct electronically. Broad interpretation of the term agreement is necessary to assure that this Act has the widest possible application consistent with its purpose of removing barriers to electronic commerce.

1. This section makes clear that this Act is intended to facilitate the use of electronic means, but does not require the use of electronic records and signatures. This fundamental principle is set forth in subsection (a) and elaborated by subsections (b) and (c), which require an intention to conduct transactions electronically and preserve the right of a party to refuse to use electronics in any subsequent transaction.

2. The paradigm of this Act is two willing parties doing transactions electronically. It is therefore appropriate that the Act is voluntary and preserves the greatest possible party autonomy to refuse electronic transactions. The requirement
that party agreement be found from all the surrounding circumstances is a limitation on the scope of this Act.

3. If this Act is to serve to facilitate electronic transactions, it must be applicable under circumstances not rising to a full fledged contract to use electronics. While absolute certainty can be accomplished by obtaining an explicit contract before relying on electronic transactions, such an explicit contract should not be necessary before one may feel safe in conducting transactions electronically. Indeed, such a requirement would itself be an unreasonable barrier to electronic commerce, at odds with the fundamental purpose of this Act. Accordingly, the requisite agreement, express or implied, must be determined from all available circumstances and evidence.

4. Subsection (b) provides that the Act applies to transactions in which the parties have agreed to conduct the transaction electronically. In this context it is essential that the parties’ actions and words be broadly construed in determining whether the requisite agreement exists. Accordingly, the Act expressly provides that the party’s agreement is to be found from all circumstances, including the parties’ conduct. The critical element is the intent of a party to conduct a transaction electronically. Once that intent is established, this Act applies. See Restatement 2d Contracts, Sections 2, 3, and 19.

Examples of circumstances from which it may be found that parties have reached an agreement to conduct transactions electronically include the following:

A. Automaker and supplier enter into a Trading Partner Agreement setting forth the terms, conditions and methods for the conduct of business between them electronically.

B. Joe gives out his business card with his business e-mail address. It may be reasonable, under the circumstances, for a recipient of the card to infer that Joe has agreed to communicate electronically for business purposes. However, in the absence of additional facts, it would not necessarily be reasonable to infer Joe’s agreement to communicate electronically for purposes outside the scope of the business indicated by use of the business card.

C. Sally may have several e-mail addresses – home, main office, office of a non-profit organization on whose board Sally sits. In each case, it may be reasonable to infer that Sally is willing to communicate electronically with respect to business related to the business/purpose associated with the respective e-mail addresses. However, depending on the circumstances, it may not be reasonable to communicate with Sally for purposes other than those related to the purpose for which she maintained a particular e-mail account.
D. Among the circumstances to be considered in finding an agreement would be the time when the assent occurred relative to the timing of the use of electronic communications. If one orders books from an on-line vendor, such as Bookseller.com, the intention to conduct that transaction and to receive any correspondence related to the transaction electronically can be inferred from the conduct. Accordingly, as to information related to that transaction it is reasonable for Bookseller to deal with the individual electronically.

The examples noted above are intended to focus the inquiry on the party’s agreement to conduct a transaction electronically. Similarly, if two people are at a meeting and one tells the other to send an e-mail to confirm a transaction – the requisite agreement under subsection (b) would exist. In each case, the use of a business card, statement at a meeting, or other evidence of willingness to conduct a transaction electronically must be viewed in light of all the surrounding circumstances with a view toward broad validation of electronic transactions.

5. Just as circumstances may indicate the existence of agreement, express or implied from surrounding circumstances, circumstances may also demonstrate the absence of true agreement. For example:

A. If Automaker, Inc. 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, notwithstanding a clause in a paper purchase contract by which the buyer agreed to receive such notices in such a manner.

B. Buyer executes a standard form contract in which an agreement to receive all notices electronically in set forth on page 3 in the midst of other fine print. Buyer has never communicated with Seller electronically, and has not provided any other information in the contract to suggest a willingness to deal electronically. Not only is it unlikely that any but the most formalistic of agreements may be found, but nothing in this Act prevents courts from policing such form contracts under common law doctrines relating to contract formation, unconscionability and the like.

6. Subsection (c) has been added to make clear the ability of a party to refuse to conduct a transaction electronically, even if the person has conducted transactions electronically in the past. The effectiveness of a party’s refusal to conduct a transaction electronically will be determined under other applicable law in light of all surrounding circumstances. Such circumstances must include an assessment of the transaction involved.
A party’s right to decline to act electronically under a specific contract, on the ground that each action under that contract amounts to a separate “transaction,” must be considered in light of the purpose of the contract and the action to be taken electronically. For example, under a contract for the purchase of goods, the giving and receipt of notices electronically, as provided in the contract, should not be viewed as discreet transactions. Rather such notices amount to separate actions which are part of the “transaction” of purchase evidenced by the contract. Allowing one party to require a change of medium in the middle of the transaction evidenced by that contract is not the purpose of this subsection. Rather this subsection is intended to preserve the party’s right to conduct the next purchase in a non-electronic medium.

7. Subsection (e) is an essential provision in the overall scheme of this Act. While this Act validates and effectuates electronic records and electronic signatures, the legal effect of such records and signatures is left to existing substantive law outside this Act except in very narrow circumstances. See, e.g., Section 16. Even when this Act operates to validate records and signatures in an electronic medium, it expressly preserves the substantive rules of other law applicable to such records. See, e.g., Section 11.

For example, beyond validation of records, signatures and contracts based on the medium used, Section 7 (a) and (b) should not be interpreted as establishing the legal effectiveness of any given record, signature or contract. Where a rule of law requires that the record contain minimum substantive content, the legal effect of such a record will depend on whether the record meets the substantive requirements of other applicable law.

Section 8 expressly preserves a number of legal requirements in currently existing law relating to the presentation of information in writing. Although this Act now would allow such information to be presented in an electronic record, Section 8 provides that the other substantive requirements of law must be satisfied in the electronic medium as well.

SECTION 6. CONSTRUCTION AND APPLICATION. This [Act] must be construed and applied:

(1) to facilitate electronic transactions consistent with other applicable law;

(2) to be consistent with reasonable practices concerning electronic transactions and with the continued expansion of those practices; and
(3) to effectuate its general purpose to make uniform the law with respect to
the subject of this [Act] among States enacting it.

Comment

1. 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.

2. This Act has been drafted to permit flexible application consistent with
its purpose to validate electronic transactions. The provisions of this Act validating
and effectuating the employ of electronic media allow the courts to apply them to
new and unforeseen technologies and practices. As time progresses, it is
anticipated that what is new and unforeseen today will be commonplace tomorrow.
Accordingly, this legislation is intended to set a framework for the validation of
media which may be developed in the future and which demonstrate the same
qualities as the electronic media contemplated and validated under this Act.
SECTION 7. LEGAL RECOGNITION OF ELECTRONIC RECORDS, ELECTRONIC SIGNATURES, AND ELECTRONIC CONTRACTS.

(a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

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

(c) If a law requires a record to be in writing, an electronic record satisfies the law.

(d) If a law requires a signature, an electronic signature satisfies the law.

Source: UNCITRAL Model Law on Electronic Commerce, Articles 5, 6, and 7.

Comment

1. This section sets forth the fundamental premise of this Act: namely, that the medium in which a record, signature, or contract is created, presented or retained does not affect its legal significance. Subsections (a) and (b) are designed to eliminate the single element of medium as a reason to deny effect or enforceability to a record, signature, or contract. The fact that the information is set forth in an electronic, as opposed to paper, record is irrelevant.

2. Under Restatement 2d Contracts Section 8, a contract may have legal effect and yet be unenforceable. Indeed, one circumstance where a record or contract may have effect but be unenforceable is in the context of the Statute of Frauds. Though a contract may be unenforceable, the records may have collateral effects, as in the case of a buyer that insures goods purchased under a contract unenforceable under the Statute of Frauds. The insurance company may not deny a claim on the ground that the buyer is not the owner, though the buyer may have no direct remedy against the seller for failure to deliver. See Restatement 2d Contracts, Section 8, Illustration 4.

While this section would validate an electronic record for purposes of a statute of frauds, if an agreement to conduct the transaction electronically cannot reasonably be found (See Section 5(b)) then a necessary predicate to the applicability of this Act would be absent and this Act would not validate the
electronic record. Whether the electronic record might be valid under other law is not addressed by this Act.

3. Subsections (c) and (d) provide the positive assertion that electronic records and signatures satisfy legal requirements for writings and signatures. The provisions are limited to requirements in laws that a record be in writing or be signed. This section does not address requirements imposed by other law in addition to requirements for writings and signatures. See, e.g., Section 8.

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

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

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

4. Section 8 addresses additional requirements imposed by other law which may affect the legal effect or enforceability of an electronic record in a particular case. For example, in Section 8(a) the legal requirement addressed is the provision of information in writing. The section then sets forth the standards to be applied in determining whether the provision of information by an electronic record is the equivalent of the provision of information in writing. The requirements in Section 8 are in addition to the bare validation that occurs under this section.

5. Under the substantive law applicable to a particular transaction within this Act, the legal effect 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 (See Section 15). An electronic record attributed to a party under Section 9 and complying with the requirements of Section 15 would suffice in that case, notwithstanding that it may not contain an electronic signature.

**SECTION 8. PROVISION OF INFORMATION IN WRITING;**

**PRESENTATION OF RECORDS.**

(a) If parties have agreed to conduct a transaction by electronic means and a law requires a person to provide, send, or deliver information in writing to another person, the requirement is satisfied if the information is provided, sent, or delivered, as the case may be, in an electronic record capable of retention by the recipient at the time of receipt. An electronic record is not capable of retention by the recipient if the sender or its information processing system inhibits the ability of the recipient to print or store the electronic record.

(b) If a law other than this [Act] requires a record (i) to be posted or displayed in a certain manner, (ii) to be sent, communicated, or transmitted by a specified method, or (iii) to contain information that is formatted in a certain manner, the following rules apply:

(1) The record must be posted or displayed in the manner specified in the other law.

(2) Except as otherwise provided in subsection (d)(2), the record must be sent, communicated, or transmitted by the method specified in the other law.

(3) The record must contain the information formatted in the manner specified in the other law.
(c) If a sender inhibits the ability of a recipient to store or print an electronic record, the electronic record is not enforceable against the recipient.

(d) The requirements of this section may not be varied by agreement, but:

(1) to the extent a law other than this [Act] requires information to be provided, sent, or delivered in writing but permits that requirement to be varied by agreement, the requirement under subsection (a) that the information be in the form of an electronic record capable of retention may also be varied by agreement; and

(2) a requirement under a law other than this [Act] to send, communicate, or transmit a record by [first-class mail, postage prepaid] [regular United States mail], may be varied by agreement to the extent permitted by the other law.

Source: Canadian – Uniform Electronic Commerce Act

Comment

1. This section is a savings provision, designed to assure, consistent with the fundamental purpose of this Act, that otherwise applicable substantive law will not be overridden by this Act. The section makes clear that while the pen and ink provisions of such other law may be satisfied electronically, nothing in this Act vitiates the other requirements of such laws. The section addresses a number of issues related to disclosures and notice provisions in other laws.

2. This section is independent of the prior section. Section 7 refers to legal requirements for a writing. This section refers to legal requirements for the provision of information in writing or relating to the method or manner of presentation or delivery of information. The section addresses more specific legal requirements of other laws, provides standards for satisfying the more particular legal requirements, and defers to other law for satisfaction of requirements under those laws.

3. Under subsection (a), to meet a requirement of other law that information be provided in writing, the recipient of an electronic record of the information must be able to get to the electronic record and read it, and must have the ability to get
back to the information in some way at a later date. Accordingly, the section requires that the electronic record be capable of retention for later review.

The section specifically provides that any inhibition on retention imposed by the sender or the sender’s system will preclude satisfaction of this section. Use of technological means now existing or later developed which prevents the recipient from retaining a copy of the information would result in a determination that information has not been provided under subsection (a). The policies underlying laws requiring the provision of information in writing warrant the imposition of an additional burden on the sender to make the information available in a manner which will permit subsequent reference. A difficulty does exist for senders of information because of the disparate systems of their recipients and the capabilities of those systems. However, in order to satisfy the legal requirement of other law to make information available, the sender must assure that the recipient receives and can retain the information. However, it is left for the courts to determine whether the sender has complied with this subsection if evidence demonstrates that it is something peculiar the recipient’s system which precludes subsequent reference to the information.

4. Subsection (b) is a savings provision for laws which provide for the means of delivering or displaying information and which are not affected by the Act. For example, if a law requires delivery of notice by first class US mail, that means of delivery would not be affected by this Act. The information to be delivered may be provided on a disc, i.e., in electronic form, but the particular means of delivery must still be via the US postal service. Display, delivery and formatting requirements will continue to be applicable to electronic records and signatures. If those legal requirements can be satisfied in an electronic medium, e.g., the information can be presented in the equivalent of 20 point bold type as required by other law, this Act will validate the use of the medium, leaving to the other applicable law the question of whether the particular electronic record meets the other legal requirements. If a law requires that particular records be delivered together, or attached to other records, this Act does not preclude the delivery of the records together in an electronic communication, so long as the records are connected or associated with each other in a way determined to satisfy the other law.

5. Subsection (c) provides incentives for senders of information to use systems which will not inhibit the other party from retaining the information. However, there are circumstances where a party providing certain information may wish to inhibit retention in order to protect intellectual property rights or prevent the other party from retaining confidential information about the sender. In such cases inhibition is understandable, but if the sender wishes to enforce the record in which the information is contained, the sender may not inhibit its retention by the
recipient. Unlike subsection (a), subsection (c) applies in all transactions and simply provides for unenforceability against the recipient. Subsection (a) applies only where another law imposes the writing requirement, and subsection (a) imposes a broader responsibility on the sender to assure retention capability by the recipient.

6. The protective purposes of this section justify the non-waivability provided by subsection (d). However, since the requirements for sending and formatting and the like are imposed by other law, to the extent other law permits waiver of such protections, there is no justification for imposing a more severe burden in an electronic environment.

SECTION 9. ATTRIBUTION AND EFFECT OF ELECTRONIC RECORD AND ELECTRONIC SIGNATURE.

(a) An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.

(b) The effect of an electronic record or electronic signature attributed to a person under subsection (a) is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties’ agreement, if any, and otherwise as provided by law.

Comment

1. Under subsection (a), so long as the electronic record or electronic signature resulted from a person’s action it will be attributed to that person – the legal effect of that attribution is addressed in subsection (b). This section does not alter existing rules of law regarding attribution. The section assures that such rules will be applied in the electronic environment. A person’s actions include actions taken by human agents of the person, as well as actions taken by an electronic agent, i.e., the tool, of the person. Although the rule may appear to state the obvious, it assures that the record or signature is not ascribed to a machine, as opposed to the person operating or programing the machine.
In each of the following cases, both the electronic record and electronic signature would be attributable to a person under subsection (a):

A. The person types his/her name as part of an e-mail purchase order;

B. The person’s employee, pursuant to authority, types the person’s name as part of an e-mail purchase order;

C. The person’s computer, programmed to order goods upon receipt of inventory information within particular parameters, issues a purchase order which includes the person’s name, or other identifying information, as part of the order.

In each of the above cases, law other than this Act would ascribe both the signature and the action to the person if done in a paper medium. Subsection (a) expressly provides that the same result will occur when an electronic medium is used.

2. Nothing in this section affects the use of a signature as a device for attributing a record to a person. Indeed, a signature is often the primary method for attributing a record to a person. In the foregoing examples, once the electronic signature is attributed to the person, the electronic record would also be attributed to the person, unless the person established fraud, forgery, or other invalidating cause. However, a signature is not the only method for attribution.

3. The use of facsimile transmissions provides a number of examples of attribution using information other than a signature. A facsimile may be attributed to a person because of the information printed across the top of the page that indicates the machine from which it was sent. Similarly, the transmission may contain a letterhead which identifies the sender. Some cases have held that the letterhead actually constituted a signature because it was a symbol adopted by the sender with intent to authenticate the facsimile. However, the signature determination resulted from the necessary finding of intention in that case. Other cases have found facsimile letterheads NOT to be signatures because the requisite intention was not present. The critical point is that with or without a signature, information within the electronic record may well suffice to provide the facts resulting in attribution of an electronic record to a particular party.

In the context of attribution of records, normally the content of the record will provide the necessary information for a finding of attribution. It is also possible that an established course of dealing between parties may result in a finding of attribution. Just as with a paper record, evidence of forgery or counterfeiting may be introduced to rebut the evidence of attribution.
4. Certain information may be present in an electronic environment that does not appear to attribute but which clearly links a person to a particular record. Numerical codes, personal identification numbers, public and private key combinations all serve to establish the party to whom an electronic record should be attributed. Of course security procedures will be another piece of evidence available to establish attribution.

The inclusion of a specific reference to security procedures as a means of proving attribution is salutary because of the unique importance of security procedures in the electronic environment. In certain processes, a technical and technological security procedure may be the best way to convince a trier of fact that a particular electronic record or signature was that of a particular person. In certain circumstances, the use of a security procedure to establish that the record and related signature came from the person’s business might be necessary to overcome a claim that a hacker intervened. The reference to security procedures is not intended to suggest that other forms of proof of attribution should be accorded less persuasive effect. It is also important to recall that the particular strength of a given procedure does not affect the procedure’s status as a security procedure, but only affects the weight to be accorded the evidence of the security procedure as tending to establish attribution.

5. This section does apply in determining the effect of a “click-through” transaction. A “click-through” transaction involves a process which, if executed with an intent to “sign,” will be an electronic signature. See definition of Electronic Signature. In the context of an anonymous “click-through,” issues of proof will be paramount. This section will be relevant to establish that the resulting electronic record is attributable to a particular person upon the requisite proof, including security procedures which may track the source of the click-through.

6. Once it is established that a record or signature is attributable to a particular party, the effect of a record or signature must be determined in light of the context and surrounding circumstances, including the parties’ agreement, if any. Also informing the effect of any attribution will be other legal requirements considered in light of the context. Subsection (b) addresses the effect of the record or signature once attributed to a person.

**SECTION 10. EFFECT OF CHANGE OR ERROR.** If a change or error in an electronic record occurs in a transmission between parties to a transaction, the following rules apply:
(1) If the parties have agreed to use a security procedure to detect changes or errors and one party has conformed to the procedure, but the other party has not, and the nonconforming party would have detected the change or error had that party also conformed, the conforming party may avoid the effect of the changed or erroneous electronic record.

(2) In an automated transaction involving an individual, the individual may avoid the effect of an electronic record that resulted from an error made by the individual in dealing with the electronic agent of another person if the electronic agent did not provide an opportunity for the prevention or correction of the error and, at the time the individual learns of the error, the individual:

(A) promptly notifies the other person of the error and that the individual did not intend to be bound by the electronic record received by the other person;

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

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

(3) If neither paragraph (1) nor paragraph (2) applies, the change or error has the effect provided by other law, including the law of mistake, and the parties’ contract, if any.
(4) Paragraphs (2) and (3) may not be varied by agreement.

Source: Restatement 2d Contracts, Sections 152-155.

Comment

1. This section is limited to changes and errors occurring in transmissions between parties – whether person-person (paragraph 1) or in an automated transaction involving an individual and a machine (paragraphs 1 and 2). The section focuses on the effect of changes and errors occurring when records are exchanged between parties. In cases where changes and errors occur in contexts other than transmission, the law of mistake is expressly made applicable to resolve the conflict.

   The section covers both changes and errors. For example, if Buyer sends a message to Seller ordering 100 widgets, but Buyer’s information processing system changes the order to 1000 widgets, a “change” has occurred between what Buyer transmitted and what Seller received. If on the other hand, Buyer typed in 1000 intending to order only 100, but sent the message before noting the mistake, an error would have occurred which would also be covered by this section.

2. Paragraph (1) deals with any transmission where the parties have agreed to use a security procedure to detect changes and errors. It operates against the non-conforming party, i.e., the party in the best position to have avoided the change or error, regardless of whether that person is the sender or recipient. The source of the error/change is not indicated, and so both human and machine errors/changes would be covered. With respect to errors or changes that would not be detected by the security procedure even if applied, the parties are left to the general law of mistake to resolve the dispute.

3. Paragraph (1) applies only in the situation where a security procedure would detect the error/change but one party fails to use the procedure and does not detect the error/change. In such a case, consistent with the law of mistake generally, the record is made avoidable at the instance of the party who took all available steps to avoid the mistake. See Restatement 2d Contracts Sections 152-154.

   Making the erroneous record avoidable by the conforming party is consistent with Sections 153 and 154 of the Restatement 2d Contracts because the non-conforming party was in the best position to avoid the problem, and would bear the risk of mistake. Such a case would constitute mistake by one party. The mistaken party (the conforming party) would be entitled to avoid any resulting contract under Section 153 because s/he does not have the risk of mistake and the non-conforming party had reason to know of the mistake.
4. As with paragraph (1), paragraph (2), when applicable, allows the mistaken party to avoid the effect of the erroneous electronic record. However, the subsection is limited to human error on the part of an individual when dealing with the electronic agent of the other party. In a transaction between individuals there is a greater ability to correct the error before parties have acted on it. However, when an individual makes an error while dealing with the electronic agent of the other party, it may not be possible to correct the error before the other party has shipped or taken other action in reliance on the erroneous record.

Paragraph (2) applies only to errors made by individuals. If the error results from the electronic agent, it would constitute a system error. In such a case the effect of that error would be resolved under paragraph (1) if applicable, otherwise under paragraph (3) and the general law of mistake.

5. The party acting through the electronic agent/machine is given incentives by this section to build in safeguards which enable the individual to prevent the sending of an erroneous record, or correct the error once sent. For example, the electronic agent may be programmed to provide a “confirmation screen” to the individual setting forth all the information the individual initially approved. This would provide the individual with the ability to prevent the erroneous record from ever being sent. Similarly, the electronic agent might receive the record sent by the individual and then send back a confirmation which the individual must again accept before the transaction is completed. This would allow for correction of an erroneous record. In either case, the electronic agent would “provide an opportunity for prevention or correction of the error,” and the subsection would not apply. Rather, the effect of any error is governed by other law.

6. Paragraph (2) also places additional requirements on the mistaken individual before the paragraph may be invoked to avoid an erroneous electronic record. The individual must take prompt action to advise the other party of the error and the fact that the individual did not intend the electronic record. Whether the action is prompt must be determined from all the circumstances including the individual’s ability to contact the other party. The individual should advise the other party both of the error and of the lack of intention to be bound (i.e., avoidance) by the electronic record received. Since this provision allows avoidance by the mistaken party, that party should also be required to expressly note that it is seeking to avoid the electronic record, i.e., lacked the intention to be bound.

Second, restitution is normally required in order to undo a mistaken transaction. Accordingly, the individual must also return or destroy any consideration received, adhering to instructions from the other party in any case. This is to assure that the other party retains control over the consideration sent in error.
Finally, and most importantly in regard to transactions involving intermediaries which may be harmed because transactions cannot be unwound, the individual cannot have received any benefit from the transaction. This section prevents a party from unwinding a transaction after the delivery of value and consideration which cannot be returned or destroyed. For example, if the consideration received is information, it may not be possible to avoid the benefit conferred. While the information itself could be returned, mere access to the information, or the ability to redistribute the information would constitute a benefit precluding the mistaken party from unwinding the transaction. It may also occur that the mistaken party receives consideration which changes in value between the time of receipt and the first opportunity to return. In such a case restitution cannot be made adequately, and the transaction would not be avoidable. In each of the foregoing cases, under subparagraph (2)(c), the individual would have received the benefit of the consideration and would NOT be able to avoid the erroneous electronic record under this section.

7. In all cases not covered by paragraphs (1) or (2), where error or change to a record occur, the parties contract, or other law, specifically including the law of mistake, applies to resolve any dispute. In the event that the parties’ contract and other law would achieve different results, the construction of the parties’ contract is left to the other law. If the error occurs in the context of record retention, Section 12 will apply. In that case the standard is one of accuracy and retrievability of the information.

8. Paragraph (4) makes the error correction provision in paragraph (2) and the application of the law of mistake in paragraph (3) non-variable. Paragraph (2) provides incentives for parties using electronic agents to establish safeguards for individuals dealing with them. It also avoids unjustified windfalls to the individual by erecting stringent requirements before the individual may exercise the right of avoidance under the paragraph. Therefore, there is no reason to permit parties to avoid the paragraph by agreement. Rather, parties should satisfy the paragraph’s requirements.

SECTION 11. NOTARIZATION AND ACKNOWLEDGMENT. If a law requires a signature or record to be notarized, acknowledged, verified, or made under oath, the requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be
included by other applicable law, is attached to or logically associated with the signature or record.

**Comment**

This section permits a notary public and other authorized officers to act electronically, effectively removing the stamp/seal requirements. However, the section does not eliminate any of the other requirements of notarial laws, and consistent with the entire thrust of this Act, simply allows the signing and information to be accomplished in an electronic medium.

For example, Buyer wishes to send a notarized Real Estate Purchase Agreement to Seller via e-mail. The notary must appear in the room with the Buyer, satisfy him/herself as to the identity of the Buyer, and swear to that identification. All that activity must be reflected as part of the electronic Purchase Agreement and the notary’s electronic signature must appear as a part of the electronic real estate purchase contract.

As another example, Buyer seeks to send Seller an affidavit averring defects in the products received. A court clerk, authorized under state law to administer oaths, is present with Buyer in a room. The Clerk administers the oath and includes the statement of the oath, together with any other requisite information, in the electronic record to be sent to the Seller. Upon administering the oath and witnessing the application of Buyer’s electronic signature to the electronic record, the Clerk also applies his electronic signature to the electronic record. So long as all substantive requirements of other applicable law have been fulfilled and are reflected in the electronic record, the sworn electronic record of Buyer is as effective as if it had been transcribed on paper.

**SECTION 12. RETENTION OF ELECTRONIC RECORDS; ORIGINALS.**

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

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

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

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

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

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

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

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


Comment

1. This section deals with the serviceability of electronic records as retained records and originals. 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). This section assures that information stored electronically will remain effective for all audit, evidentiary, archival and similar purposes.

2. In an electronic medium, the concept of an original document is problematic. For example, as one drafts a document on a computer the “original” is either on a disc or the hard drive to which the document has been initially saved. If one periodically saves the draft, the fact is that at times a document may be first saved to disc then to hard drive, and at others vice versa. In such a case the “original” may change from the information on the disc to the information on the hard drive. Indeed, 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, in the context of record retention, the concern focuses on the integrity of the information, and not with its “originality.”

3. Subsection (a) requires accuracy and the ability to access at a later time. The requirement of accuracy is derived from the Uniform and Federal Rules of Evidence. The requirement of continuing accessibility addresses the issue of technology obsolescence and the need to update and migrate information to developing systems. It is not unlikely that within the span of 5-10 years (a period during which retention of much information is required) a corporation may evolve through one or more generations of technology. More to the point, this technology may be incompatible with each other necessitating the reconversion of information from one system to the other.

For example, certain operating systems from the early 1980’s, e.g., memory typewriters, became obsolete with the development of personal computers. The information originally stored on the memory typewriter would need to be converted to the personal computer system in a way meeting the standards for accuracy contemplated by this section. It is also possible that the medium on which the information is stored is less stable. For example, information stored on floppy discs is generally less stable, and subject to a greater threat of disintegration, that information stored on a computer hard drive. In either case, the continuing accessibility issue must be satisfied to validate information stored by electronic means under this section.

This section permits 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.
The subsection refers to the information contained in an electronic record, rather than relying on the term electronic record, as a matter of clarity that the critical aspect in retention is the information itself. What information must be retained is determined by the purpose for which the information is needed. If the addressing and pathway information regarding an e-mail is relevant, then that information should also be retained. However if it is the substance of the e-mail that is relevant, only that information need be retained. Of course, wise record retention would include all such information since what information will be relevant at a later time will not be known.

4. Subsections (b) and (c) simply make clear that certain ancillary information or the use of third parties, does not affect the serviceability of records and information retained electronically. Again, the relevance of particular information will not be known until that information is required at a subsequent time.

5. Subsection (d) continues the theme of the Act as validating electronic records as originals where the law requires retention of an original. The validation of electronic records and electronic information as originals is consistent with the Uniform Rules of Evidence. See Uniform Rules of Evidence 1001(3), 1002, 1003 and 1004.

6. Subsection (e) specifically addresses particular concerns regarding check retention statutes in many jurisdictions. A Report compiled by the Federal Reserve Bank of Boston identifies hundreds of state laws which require the retention or production of original canceled checks. Such requirements preclude banks and their customers from realizing the benefits and efficiencies related to truncation processes otherwise validated under current law. The benefits to banks and their customers from electronic check retention are effectuated by this provision.

7. Subsections (f) and (g) generally address other record retention statutes. As with check retention, all businesses and individuals may realize significant savings from electronic record retention. So long as the standards in Section 12 are satisfied, this section permits all parties to obtain those benefits. As always the government may require records in any medium, however, these subsections require a governmental agency to specifically identify the types of records and requirements that will be imposed.
SECTION 13. ADMISSIBILITY IN EVIDENCE. In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.

Source: UNCITRAL Model Law on Electronic Commerce Article 9.

Comment

Like Section 7, this section prevents the nonrecognition of electronic records and signatures solely on the ground of the media in which information is presented.

Nothing in this section relieves a party from establishing the necessary foundation for the admission of an electronic record. See Uniform Rules of Evidence 1001(3), 1002, 1003 and 1004.

SECTION 14. AUTOMATED TRANSACTION. In an automated transaction, the following rules apply:

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

(2) A contract may be formed by the interaction of an electronic agent and an individual, acting on the individual’s own behalf or for another person, including by an interaction in which the individual performs actions that the individual is free to refuse to perform and which the individual knows or has reason to know will cause the electronic agent to complete the transaction or performance.

(3) The terms of the contract are determined by the substantive law applicable to it.

Source: UNCITRAL Model Law on Electronic Commerce Article 11.
Comment

1. This section confirms that contracts can be formed by machines functioning as electronic agents for parties to a transaction. It negates any claim that lack of human intent, at the time of contract formation, prevents contract formation. When machines are involved, the requisite intention flows from the programming and use of the machine. As in other cases, these are salutary provisions consistent with the fundamental purpose of the Act to remove barriers to electronic transactions while leaving the substantive law, e.g., law of mistake, law of contract formation, unaffected to the greatest extent possible.

2. The process in paragraph (2) validates an anonymous click-through transaction. It is possible that an anonymous click-through process may simply result in no recognizable legal relationship, e.g., A goes to a person’s website and acquires access without in any way identifying herself, or otherwise indicating agreement or assent to any limitation or obligation, and the owner’s site grants A access. In such a case no legal relationship has been created.

On the other hand it may be possible that A’s actions indicate agreement to a particular term. For example, A goes to a website and is confronted by an initial screen which advises her that the information at this site is proprietary, that A may use the information for her own personal purposes, but that, by clicking below, A agrees that any other use without the site owner’s permission is prohibited. If A clicks “agree” and downloads the information and then uses the information for other, prohibited purposes, should not A be bound by the click? It seems the answer properly should be, and would be, yes.

If the owner can show that the only way A could have obtained the information was from his website, and that the process to access the subject information required that A must have clicked the “I agree” button after having the ability to see the conditions on use, A has performed actions which A was free to refuse, which A knew would cause the site to grant her access, i.e., “complete the transaction.” The terms of the resulting contract will be determined under general contract principles, but will include the limitation on A’s use of the information, as a condition precedent to granting her access to the information.

3. In the transaction set forth in Comment 2, the record of the transaction also will include an electronic signature. By clicking “I agree” A adopted a process with the intent to “sign,” i.e., bind herself to a legal obligation, the resulting record of the transaction. If a “signed writing” were required under otherwise applicable law, this transaction would be enforceable. If a “signed writing” were not required, it may be sufficient to establish that the electronic record is attributable to A under Section 9. Attribution may be shown in any manner reasonable including showing
that, of necessity, A could only have gotten the information through the process at the website.

SECTION 15. TIME AND PLACE OF SENDING AND RECEIPT.

(a) Unless otherwise agreed between the sender and the recipient, an electronic record is sent when it:

(1) is addressed properly or otherwise directed properly to an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record;

(2) is in a form capable of being processed by that system; and

(3) enters an information processing system outside the control of the sender or of a person that sent the electronic record on behalf of the sender or enters a region of the information processing system designated or used by the recipient which is under the control of the recipient.

(b) Unless otherwise agreed between a sender and the recipient, an electronic record is received when:

(1) it enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record; and

(2) it is in a form capable of being processed by that system.
(c) Subsection (b) applies even if the place the information processing system is located is different from the place the electronic record is deemed to be received under subsection (d).

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

(1) If the sender or recipient has more than one place of business, the place of business of that person is the place having the closest relationship to the underlying transaction.

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

(e) An electronic record is received under subsection (b) even if no individual is aware of its receipt.

(f) Receipt of an electronic acknowledgment from an information processing system described in subsection (b) establishes that a record was received but, by itself, does not establish that the content sent corresponds to the content received.

(g) If a person is aware that an electronic record purportedly sent under subsection (a), or purportedly received under subsection (b), was not actually sent or received, the legal effect of the sending or receipt is determined by other
applicable law. Except to the extent permitted by the other law, the requirements of this subsection may not be varied by agreement.

**Source:** UNCITRAL Model Law on Electronic Commerce Article 15.

**Comment**

1. This section provides default rules regarding when and from where an electronic record is sent and when and where an electronic record is received. This section does not address the efficacy of the record that is sent or received. That is, whether a record is unintelligible or unusable by a recipient is a separate issue from whether that record was sent or received. The effectiveness of an illegible record, whether it binds any party, are questions left to other law.

2. Subsection (a) furnishes rules for determining when an electronic record is sent. The effect of the sending and its import are determined by other law once it is determined that a sending has occurred.

In order to have a proper sending, the subsection requires that information be properly addressed or otherwise directed to the recipient. In order to send within the meaning of this section, there must be specific information which will direct the record to the intended recipient. Although mass electronic sending is not precluded, a general broadcast message, sent to systems rather than individuals, would not suffice as a sending.

The record will be considered sent once it leaves the control of the sender, or comes under the control of the recipient. Records sent through e-mail or the internet will pass through many different server systems. Accordingly, the critical element when more than one system is involved is the loss of control by the sender.

However, the structure of many message delivery systems is such that electronic records may actually never leave the control of the sender. For example, within a university or corporate setting, e-mail sent within the system to another faculty member is technically not out of the sender’s control since it never leaves the organization’s server. Accordingly, to qualify as a sending, the e-mail must arrive at a point where the recipient has control. This section does not address the effect of an electronic record that is thereafter “pulled back,” e.g., removed from a mailbox. The analog in the paper world would be removing a letter from a person’s mailbox. As in the case of providing information electronically under Section 8, the recipient’s ability to receive a message should be judged from the perspective of whether the sender has done any action which would preclude retrieval. This is especially the case in regard to sending, since the sender must direct the record to a system designated or used by the recipient.
3. Subsection (b) provides simply that when a record enters the system which the recipient has designated or uses and to which it has access, in a form capable of being processed by that system, it is received. Keying receipt to a system accessible by the recipient removes the potential for a recipient leaving messages with a server or other service in order to avoid receipt. However, the section does not resolve the issue of how the sender proves the time of receipt.

To assure that the recipient retains control of the place of receipt, subsection (b) requires that the system be specified or used by the recipient, and that the system be used or designated for the type of record being sent. Many people have multiple e-mail addresses for different purposes. Subsection (b) assures that recipients can designate the e-mail address or system to be used in a particular transaction. For example, the recipient retains the ability to designate a home e-mail for personal matters, work e-mail for official business, or a separate organizational e-mail solely for the business purposes of that organization. If A sends B a notice at his home which relates to business, it may not be deemed received if B designated his business address as the sole address for business purposes. Whether actual knowledge upon seeing it at home would qualify as receipt is determined under the otherwise applicable substantive law.

4. Subsections (c) and (d) provide default rules for determining where a record will be considered to have been sent or received. The focus is on the place of business of the recipient and not the physical location of the information processing system, which may bear absolutely no relation to the transaction between the parties. 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 under other applicable law, e.g., conflict of laws issues, tax issues, the relevant location should be the location of the sender or recipient and not the location of the information processing system.

Subsection (d) assures individual flexibility in designating the place from which a record will be considered sent or at which a record will be considered received. Under subsection (d) a person may designate the place of sending or receipt unilaterally in an electronic record. This ability, as with the ability to designate by agreement, may be limited by otherwise applicable law to places having a reasonable relationship to the transaction.

5. Subsection (e) makes clear that receipt is not dependent on a person having notice that the record is in the person’s system. Receipt occurs when the
record reaches the designated system whether or not the recipient ever retrieves the record. The paper analog is the recipient who never reads a mail notice.

6. Subsection (f) provides legal certainty regarding the effect of an electronic acknowledgment. It only addresses the fact of receipt, not the quality of the content, nor whether the electronic record was read or “opened.”

7. Subsection (g) limits the parties’ ability to vary the method for sending and receipt provided in subsections (a) and (b), when there is a legal requirement for the sending or receipt. As in other circumstances where legal requirements derive from other substantive law, to the extent that the other law permits variation by agreement, this Act does not impose any additional requirements, and provisions of this Act may be varied to the extent provided in the other law.

SECTION 16. TRANSFERABLE RECORDS.

(a) In this section, “transferable record” means an electronic record that:

(1) would be a note under [Article 3 of the Uniform Commercial Code] or a document under [Article 7 of the Uniform Commercial Code] if the electronic record were in writing; and

(2) the issuer of the electronic record expressly has agreed is a transferable record.

(b) A person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.

(c) A system satisfies subsection (b), and a person is deemed to have control of a transferable record, if the transferable record is created, stored, and assigned in such a manner that:
(1) a single authoritative copy of the transferable record exists which is unique, identifiable, and, except as otherwise provided in paragraphs (4), (5), and (6), unalterable;

(2) the authoritative copy identifies the person asserting control as:

(A) the person to which the transferable record was issued; or

(B) if the authoritative copy indicates that the transferable record has been transferred, the person to which the transferable record was most recently transferred;

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

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

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

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

(d) Except as otherwise agreed, a person having control of a transferable record is the holder, as defined in [Section 1-201(20) of the Uniform Commercial Code], of the transferable record and has the same rights and defenses as a holder of an equivalent record or writing under [the Uniform Commercial Code], including, if the applicable statutory requirements under [Section 3-302(a), 7-501, or 9-308 of...
the Uniform Commercial Code] are satisfied, the rights and defenses of a holder in
due course, a holder to which a negotiable document of title has been duly
negotiated, or a purchaser, respectively. Delivery, possession, and indorsement are
not required to obtain or exercise any of the rights under this subsection.

(e) Except as otherwise agreed, an obligor under a transferable record has
the same rights and defenses as an equivalent obligor under equivalent records or
writings under [the Uniform Commercial Code].

(f) If requested by a person against which enforcement is sought, the person
seeking to enforce the transferable record shall provide reasonable proof that the
person is in control of the transferable record. Proof may include access to the
authoritative copy of the transferable record and related business records sufficient
to review the terms of the transferable record and to establish the identity of the
person having control of the transferable record.

Source: Revised Article 9, Section 9-105.

Comment

1. Paper negotiable instruments and documents are unique in the fact that a
tangible token – a piece of paper – actually embodies intangible rights and
obligations. The extreme difficulty of creating a unique electronic token which
embodies the singular attributes of a paper negotiable document or instrument
dictates that the rules relating to negotiable documents and instruments not be
simply amended to allow the use of an electronic record for the requisite paper
writing. However, the desirability of establishing rules by which business parties
might be able to acquire some of the benefits of negotiability in an electronic
environment is recognized by the inclusion of this section on Transferable Records.

This section provides legal support for the creation, transferability and
enforceability of electronic note and document equivalents, as against the
issuer/obligor. The certainty created by the section provides the requisite incentive
for industry to develop the systems and processes, which involve significant expenditures of time and resources, to enable the use of such electronic documents.

The importance of facilitating the development of systems which will permit electronic equivalents is a function of cost, efficiency and safety for the records. The storage cost and space needed for the billions of paper notes and documents is phenomenal. Further, natural disasters can wreak havoc on the ability to meet legal requirements for retaining, retrieving and delivering paper instruments. The development of electronic systems meeting the rigorous standards of this section will permit retention of copies which reflect the same integrity as the original. As a result storage, transmission and other costs will be reduced, while security and the ability to satisfy legal requirements governing such paper records will be enhanced.

Section 16 provides for the creation of an electronic record which may be controlled by the holder, who in turn may obtain the benefits of holder in due course and good faith purchaser status. If the benefits and efficiencies of electronic media are to be realized in this industry it is essential to establish a means by which transactions involving paper promissory notes may be accomplished completely electronically. Particularly as other aspects of such transactions are accomplished electronically, the drag on the transaction of requiring a paper note becomes evident. In addition to alleviating the logistical problems of generating, storing and retrieving paper, the mailing and transmission costs associated with such transactions will also be reduced.

2. The definition of transferable record is limited in two significant ways. First, only the equivalent of paper promissory notes and paper documents of title can be created as transferable records. Notes and Documents of Title do not impact the broad systems that relate to the broader payments mechanisms related, for example, to checks. Impacting the check collection system by allowing for “electronic checks” has ramifications well beyond the ability of this Act to address. Accordingly, this Act excludes from its scope transactions governed by UCC Articles 3 and 4. The limitation to promissory note equivalents in Section 16 is quite important in that regard because of the ability to deal with many enforcement issues by contract without affecting such systemic concerns.

Second, not only is Section 16 limited to electronic records which would qualify as negotiable promissory notes or documents if they were in writing, but the issuer of the electronic record must expressly agree that the electronic record is to be considered a transferable record. The definition of transferable record as “an electronic record that...the issuer of the electronic record expressly has agreed is a transferable record” indicates that the electronic record itself will likely set forth the issuer’s agreement, though it may be argued that a contemporaneous electronic or
written record might set forth the issuer’s agreement. However, conversion of a paper note issued as such would not be possible because the issuer would not be the issuer, in such a case, of an electronic record. The purpose of such a restriction is to assure that transferable records can only be created at the time of issuance by the obligor. The possibility that a paper note might be converted to an electronic record and then intentionally destroyed, and the effect of such action, was not intended to be covered by Section 16.

The requirement that the obligor expressly agree in the electronic record to its treatment as a transferable record does not otherwise affect the characterization of a transferable record (i.e., does not affect what would be a paper note) because it is a statutory condition. Further, it does not obligate the issuer to undertake to do any other act than the payment of the obligation evidenced by the transferable record. Therefore, it does not make the transferable record “conditional” within the meaning of Section 3-104(a)(3) of the Uniform Commercial Code.

3. Under Section 16 acquisition of “control” over an electronic record serves as a substitute for “possession” in the paper analog. More precisely, “control” under Section 16 serves as the substitute for delivery, indorsement and possession of a negotiable promissory note or negotiable document of title. Section 16(b) allows control to be found so long as “a system employed for evidencing the transfer of interests in the transferable record reliably establishes [the person claiming control] as the person to which the transferable record was issued or transferred.” The key point is that a system, whether involving third party registry or technological safeguards, must be shown to reliably establish the identity of the person entitled to payment. Section 16(c) then sets forth a safe harbor list of very strict requirements for such a system. The specific provisions listed in Section 16(c) are derived from Section 105 of Revised Article 9 of the Uniform Commercial Code. Generally, the transferable record must be unique, identifiable, and except as specifically permitted, unalterable. That “authoritative copy” must (i) identify the person claiming control as the person to whom the record was issued or most recently transferred, (ii) be maintained by the person claiming control or its designee, and (iii) be unalterable except with the permission of the person claiming control. In addition any copy of the authoritative copy must be readily identifiable as a copy and all revisions must be readily identifiable as authorized or unauthorized.

The control requirements may be satisfied through the use of a trusted third party registry system. Such systems are currently in place with regard to the transfer of securities entitlements under Article 8 of the Uniform Commercial Code, and in the transfer of cotton warehouse receipts under the program sponsored by the United States Department of Agriculture. This Act would recognize the use of such a system so long as the standards of subsection (c) were satisfied. In
addition, a technological system which met such exacting standards would also be permitted under Section 16.

For example, a borrower signs an electronic record which would be a promissory note or document if it were paper. The borrower specifically agrees in the electronic record that it will qualify as a transferable record under this section. The lender implements a newly developed technological system which dates, encrypts, and stores all the electronic information in the transferable record in a manner which lender can demonstrate reliably establishes lender as the person to which the transferable record was issued. In the alternative, the lender may contract with a third party to act as a registry for all such transferable records, retaining records establishing the party to whom the record was issued and all subsequent transfers of the record. An example of this latter method for assuring control is the system established for the issuance and transfer of electronic cotton warehouse receipts under 7 C.F.R. section 735 et seq.

Of greatest importance in the system used is the ability to securely and demonstrably be able to transfer the record to others in a manner which assures that only one “holder” exists. The need for such certainty and security resulted in the very stringent standards for a system outlined in subsection (c). A system relying on a third party registry is likely the most effective way to satisfy the requirements of subsection (c) that the transferable record remain unique, identifiable and unalterable, while also providing the means to assure that the transferee is clearly noted and identified.

It must be remembered that Section 16 was drafted in order to provide sufficient legal certainty regarding the rights of those in control of such electronic records, that legal incentives would exist to warrant the development of systems which would establish the requisite control. During the drafting of Section 16, representatives from the Federal Reserve carefully scrutinized the impact of any electronicization of any aspect of the national payment system. Section 16 represents a compromise position which, as noted, serves as a bridge pending more detailed study and consideration of what legal changes, if any, are necessary or appropriate in the context of the payment systems impacted. Accordingly, Section 16 provides limited scope for the attainment of important rights derived from the concept of negotiability, in order to permit the development of systems which will satisfy its strict requirements for control.

4. It is important to note what the section does not provide. Issues related to enforceability against intermediate transferees and transferors (i.e., indorser liability under a paper note), warranty liability that would attach in a paper note, and issues of the effect of taking a transferable record on the underlying obligation, are NOT addressed by this section. Such matters must be addressed, if at all, by
contract between and among the parties in the chain of transmission and transfer of the transferable record. In the event that such matters are not addressed by the contract, the issues would need to be resolved under otherwise applicable law. Other law may include general contract principles of assignment and assumption, or may include rules from Article 3 of the Uniform Commercial Code applied by analogy.

For example, Issuer agrees to pay a debt by means of a transferable record issued to A. Unless there is agreement between issuer and A that the transferable record “suspends” the underlying obligation (see Section 3-310 of the Uniform Commercial Code), A would not be prevented from enforcing the underlying obligation without the transferable record. Similarly, if A transfers the transferable record to B by means granting B control, B may obtain holder in due course rights against the obligor/issuer, but B’s recourse against A would not be clear unless A agreed to remain liable under the transferable record. Although the rules of Article 3 may be applied by analogy in an appropriate context, in the absence of an express agreement in the transferable record or included by applicable system rules, the liability of the transferor would not be clear.

5. Current business models exist which rely for their efficacy on the benefits of negotiability. A principal example, and one which informed much of the development of Section 16, involves the mortgage backed securities industry. Aggregators of commercial paper acquire mortgage secured promissory notes following a chain of transfers beginning with the origination of the mortgage loan by a mortgage broker. In the course of the transfers of this paper, buyers of the notes and lenders/secured parties for these buyers will intervene. For the ultimate purchaser of the paper, the ability to rely on holder in due course and good faith purchaser status creates the legal security necessary to issue its own investment securities which are backed by the obligations evidenced by the notes purchased. Only through their HIDC status can these purchasers be assured that third party claims will be barred. Only through their HIDC status can the end purchaser avoid the incredible burden of requiring and assuring that each person in the chain of transfer has waived any and all defenses to performance which may be created during the chain of transfer.

6. This section is a stand-alone provision. Although references are made to specific provisions in Article 3, Article 7, and Article 9 of the Uniform Commercial Code, these provisions are incorporated into this Act and made the applicable rules for purposes of this Act. The rights of parties to transferable records are established under subsections (d) and (e). Subsection (d) provides rules for determining the rights of a party in control of a transferable record. The subsection makes clear that the rights are determined under this section, and not under other law, by incorporating the rules on the manner of acquisition into this statute. The last
sentence of subsection (d) is intended to assure that requirements related to notions of possession, which are inherently inconsistent with the idea of an electronic record, are not incorporated into this statute.

If a person establishes control, Section 16(d) provides that that person is the “holder” of the transferable record which is equivalent to a holder of an analogous paper negotiable instrument. More importantly, if the person acquired control in a manner which would make it a holder in due course of an equivalent paper record, the person acquires the rights of a HDC. The person in control would therefore be able to enforce the transferable record against the obligor regardless of intervening claims and defenses. However, by pulling these rights into Section 16, this Act does NOT validate the wholesale electrification of promissory notes under Article 3 of the Uniform Commercial Code.

Further, it is important to understand that a transferable record under Section 16, while having no counterpart under Article 3 of the Uniform Commercial Code, would be an “account,” “general intangible,” or “payment intangible” under Article 9 of the Uniform Commercial Code. Accordingly, two separate bodies of law would apply to that asset of the obligee. A taker of the transferable record under Section 16 may acquire purchaser rights under Article 9 of the Uniform Commercial Code, however, those rights may be defeated by a trustee in bankruptcy of a prior person in control unless perfection under Article 9 of the Uniform Commercial Code by filing is achieved. If the person in control also takes control in a manner granting it holder in due course status, of course that person would take free of any claim by a bankruptcy trustee or lien creditor.

7. Subsection (e) accords to the obligor of the transferable record rights equal to those of an obligor under an equivalent paper record. Accordingly, unless a waiver of defense clause is obtained in the electronic record, or the transferee obtains HDC rights under subsection (d), the obligor has all the rights and defenses available to it under a contract assignment. Additionally, the obligor has the right to have the payment noted or otherwise included as part of the electronic record.

8. Subsection (f) grants the obligor the right to have the transferable record and other information made available for purposes of assuring the correct person to pay. This will allow the obligor to protect its interest and obtain the defense of discharge by payment or performance. This is particularly important because a person receiving subsequent control under the appropriate circumstances may well qualify as a holder in course who can enforce payment of the transferable record.

9. Section 16 is a singular exception to the thrust of this Act to simply validate electronic media used in commercial transactions. Section 16 actually provides a means for expanding electronic commerce. It provides certainty to
lenders and investors regarding the enforceability of a new class of financial services. It is hoped that the legal protections afforded by Section 16 will engender the development of technological and business models which will permit realization of the significant cost savings and efficiencies available through electronic transacting in the financial services industry. Although only a bridge to more detailed consideration of the broad issues related to negotiability in an electronic context, Section 16 provides the impetus for that broader consideration while allowing continuation of developing technological and business models.

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

Comment
See Comments following Section 19.

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

(a) Except as otherwise provided in Section 12(f), [each governmental agency] [the [designated state officer]] of this State shall determine whether, and the extent to which, [it] [a governmental agency] will send and accept electronic records and electronic signatures to and from other persons and otherwise create, generate, communicate, store, process, use, and rely upon electronic records and electronic signatures.
(b) To the extent that a governmental agency uses electronic records and electronic signatures under subsection (a), the [governmental agency] [designated state officer], giving due consideration to security, may specify:

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

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

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

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

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

Source: Illinois Act Section 25-101; Florida Electronic Signature Act, Chapter 96-324, Section 7 (1996).
Comment

See Comments following Section 19.

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


See Legislative Note below – Following Comments.

Comment

1. Sections 17-19 have been bracketed as optional provisions to be
considered for adoption by each State. Among the barriers to electronic commerce
are barriers which exist in the use of electronic media by state governmental
agencies – whether among themselves or in external dealing with the private sector.
In those circumstances where the government acts as a commercial party, e.g., in
areas of procurement, the general validation provisions of this Act will apply. That
is to say, the government must agree to conduct transactions electronically with
vendors and customers of government services.

However, there are other circumstances when government ought to establish
the ability to proceed in transactions electronically. Whether in regard to records
and communications within and between governmental agencies, or with respect to
information and filings which must be made with governmental agencies, these
sections allow a State to establish the ground work for such electronicization.

2. The provisions in Sections 17-19 are broad and very general. In many
States they will be unnecessary because enacted legislation designed to facilitate
governmental use of electronic records and communications is in place. However, in many States broad validating rules are needed and desired. Accordingly, this Act provides these sections as a baseline.

Of paramount importance in all States however, is the need for States to assure that whatever systems and rules are adopted, the systems established are compatible with the systems of other governmental agencies and with common systems in the private sector. A very real risk exists that implementation of systems by myriad governmental agencies and offices may create barriers because of a failure to consider compatibility, than would be the case otherwise.

3. The provisions in Section 17-19 are broad and general to provide the greatest flexibility and adaptation to the specific needs of the individual States. The differences and variations in the organization and structure of governmental agencies mandates this approach. However, it is imperative that each State always keep in mind the need to prevent the erection of barriers through appropriate coordination of systems and rules within the parameters set by the State.

4. Section 17 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 the section gives enacting legislatures the option to leave the decision to use electronic records or convert written records and signatures to the governmental agency or assign that duty to a designated state officer. It also authorizes the destruction of written records after conversion to electronic form.

5. Section 18 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 (c)). However, it does provide specifically that with respect to electronic records used for evidentiary purposes, Section 12 will apply unless a particular agency expressly opts out.

6. Section 19 is the most important section of the three. It requires governmental agencies or state officers to take account of consistency in applications and interoperability to the extent practicable when promulgating standards. This section is critical in addressing the concern that inconsistent applications may promote barriers greater than currently exist. Without such direction the myriad systems that could develop independently would be new barriers to electronic commerce, not a removal of barriers. The key to interoperability is flexibility and adaptability. The requirement of a single system may be as big a barrier as the proliferation of many disparate systems.
Legislative Note Regarding Adoption of Sections 17-19

1. Sections 17-19 are optional sections for consideration by individual legislatures for adoption, and have been bracketed to make this clear. The inclusion or exclusion of Sections 17-19 will not have a detrimental impact on the uniformity of adoption of this Act, so long as Sections 1-16 are adopted uniformly as presented. In some States Sections 17-19 will be unnecessary because legislation is already in place to authorize and implement government use of electronic media. However, the general authorization provided by Sections 17-19 may be critical in some States which desire to move forward in this area.

2. In the event that a state legislature chooses to adopt Sections 17-19, a number of issues must be addressed:

   A. Is the general authorization to adopt electronic media, provided by Sections 17-19 sufficient for the needs of the particular jurisdiction, or is more detailed and specific authorization necessary? This determination may be affected by the decision regarding the appropriate entity or person to oversee implementation of the use of electronic media (See next paragraph). Sections 17-19 are broad and general in the authorization granted. Certainly greater specificity can be added subsequent to adoption of these sections. The question for the legislature is whether greater direction and specificity is needed at this time. If so, the legislature should not enact Sections 17-19 at this time.

   B. Assuming a legislature decides to enact Sections 17-19, what entity or person should oversee implementation of the government’s use of electronic media? As noted in each of Sections 17-19, again by brackets, a choice must be made regarding the entity to make critical decisions regarding the systems and rules which will govern the use of electronic media by the State. Each State will need to consider its particular structure and administration in making this determination. However, legislatures are strongly encouraged to make compatibility and interoperability considerations paramount in making this determination.

   C. Finally, a decision will have to be made regarding the process by which coordination of electronic systems will occur between the various branches of state government and among the various levels of government within the State. Again this will require consideration of the unique situation in each State.

3. If a State chooses not to enact Sections 17-19, UETA Sections 1-16 will still apply to governmental entities when acting as a “person” engaging in “transactions” within its scope. The definition of transaction includes “governmental affairs.” Of course, like any other party, the circumstances surrounding a transaction must indicate that the governmental actor has agreed to
act electronically (See Section 5(b)), but otherwise all the provisions of Sections 1-16 will apply to validate the use of electronic records and signatures in transactions involving governmental entities.

If a State does choose to enact Sections 17-19, Sections 1-16 will continue to apply as above. In addition, Sections 17-19 will provide authorization for intra-governmental uses of electronic media. Finally, Sections 17-19 provide a broader authorization for the State to develop systems and procedures for the use of electronic media in its relations with non-governmental entities and persons.

**SECTION 20. SEVERABILITY CLAUSE.** If any provision of this [Act] or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this [Act] which can be given effect without the invalid provision or application, and to this end the provisions of this [Act] are severable.

**SECTION 21. EFFECTIVE DATE.** This [Act] takes effect .........................
Chapter 84 — Electronic Transactions

2015 EDITION

ELECTRONIC TRANSACTIONS

COMMERCIAL TRANSACTIONS

UNIFORM ELECTRONIC TRANSACTIONS ACT

84.001 Short title
84.004 Definitions for ORS 84.001 to 84.061
84.007 Scope
84.010 Prospective application
84.013 Use of electronic records and electronic signatures; variation by agreement
84.014 Consent for conducting transaction with governmental agency
84.016 Construction and application
84.019 Legal recognition of electronic records, electronic signatures and electronic contracts
84.022 Provision of information in writing; presentation of records
84.025 Attribution and effect of electronic record and electronic signature
84.028 Effect of change or error
84.031 Notarization and acknowledgment
84.034 Retention of electronic records; originals
84.037 Admissibility in evidence
84.040 Automated transaction
84.043 Time and place of sending and receipt
84.046 Transferable records
84.049 Creation and retention of electronic records by governmental agency; conversion of records into electronic records
84.052 Acceptance and distribution of electronic records by governmental agencies
84.055 Interoperability
84.058 Severability clause
84.061 Federal electronic signatures law partially superseded
84.063 Rules

MISCELLANEOUS PROVISIONS
UNIFORM ELECTRONIC TRANSACTIONS ACT

84.001 Short title. ORS 84.001 to 84.061 may be cited as the Uniform Electronic Transactions Act. [2001 c.535 §1]

84.004 Definitions for ORS 84.001 to 84.061. As used in ORS 84.001 to 84.061:

(1) “Agreement” means the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations and procedures given the effect of agreements under laws otherwise applicable to a particular transaction.

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

(3) “Computer program” means a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result.

(4) “Contract” means the total legal obligation resulting from the parties’ agreement under ORS 84.001 to 84.061 and other applicable law.

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

(6) “Electronic agent” means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual.

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

(8) “Electronic signature” means an electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

(9) “Governmental agency” means an executive, legislative or judicial agency, department, board, commission, authority, institution or instrumentality of the federal government or of a state or of a county, municipality or other political subdivision of a state.

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

(11) “Information processing system” means an electronic system for creating, generating, sending, receiving, storing, displaying or processing information.

(12) “Person” means an individual, corporation, business trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation or any other legal or commercial entity.

(13) “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.

(14) “Security procedure” means a procedure employed 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 information in an electronic record. “Security procedure” includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.

(15) “State” means a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands or any territory or insular possession subject to the jurisdiction of the United States. “State” includes an Indian tribe or band or an Alaskan native village, which is recognized by federal law or formally acknowledged by a state.

(16) “Transaction” means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial or governmental affairs. [2001 c.535 §2; 2009 c.294 §10]

84.007 Scope. (1) Except as otherwise provided in subsection (2) of this section, ORS 84.001 to 84.061 apply to electronic records and electronic signatures relating to a transaction.

(2) ORS 84.001 to 84.061 do not apply to a transaction to the extent it is governed by:

(a) A law governing the creation and execution of wills, codicils or testamentary trusts; or

(b) The Uniform Commercial Code other than ORS chapters 72 and 72A.

(3) ORS 84.001 to 84.061 apply to an electronic record or electronic signature otherwise excluded from the application of ORS 84.001 to 84.061 under subsection (2) of this section to the extent it is governed by a law other than those specified in subsection (2) of this section.

(4) A transaction subject to ORS 84.001 to 84.061 is also subject to other applicable substantive law. [2001 c.535 §3; 2009 c.181 §103]

84.010 Prospective application. ORS 84.001 to 84.061 apply to any electronic record or electronic signature created, generated, sent,
Chapter 1—Technology on Contracting: Practical and Legal Implications

84.013 Use of electronic records and electronic signatures; variation by agreement. (1) ORS 84.001 to 84.061 do not require a record or signature to be created, generated, sent, communicated, received, stored or otherwise processed or used by electronic means or in electronic form.

(2) ORS 84.001 to 84.061 apply only to transactions between parties, each of which has agreed to conduct transactions by electronic means. Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties’ conduct.

(3) A party that agrees to conduct a transaction by electronic means may refuse to conduct other transactions by electronic means. The right granted by this subsection may not be waived by agreement.

(4) Except as otherwise provided in ORS 84.001 to 84.061, the effect of any provision of ORS 84.001 to 84.061 may be varied by agreement. The presence in certain provisions of ORS 84.001 to 84.061 of the words “unless otherwise agreed,” or words of similar import, does not imply that the effect of other provisions of ORS 84.001 to 84.061 may not be varied by agreement.

(5) Whether an electronic record or electronic signature has legal consequences is determined by ORS 84.001 to 84.061 and other applicable law. [2001 c.535 §5]

84.014 Consent for conducting transaction with governmental agency. Notwithstanding the provisions of ORS 84.013, a governmental agency does not require an individual’s agreement or consent to conduct a transaction by electronic means or create or retain an electronic record of a transaction if the governmental agency conducts transactions by electronic means or creates, sends, accepts, generates, communicates, stores, processes, uses or relies on electronic records of transactions regularly and in the course of the governmental agency’s ordinary business. [2011 c.39 §2]

84.016 Construction and application. ORS 84.001 to 84.061 must be construed and applied:

(1) To facilitate electronic transactions consistent with other applicable law;

(2) To be consistent with reasonable practices concerning electronic transactions and with the continued expansion of those practices; and

(3) To effectuate the general purpose of ORS 84.001 to 84.061 to make uniform the law with respect to the subject of ORS 84.001 to 84.061 among states enacting it. [2001 c.535 §6]

84.019 Legal recognition of electronic records, electronic signatures and electronic contracts. (1) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

(2) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

(3) If a law requires a record to be in writing, an electronic record satisfies the law.

(4) If a law requires a signature, an electronic signature satisfies the law. [2001 c.535 §7]

84.022 Provision of information in writing; presentation of records. (1) If parties have agreed to conduct a transaction by electronic means and a law requires a person to provide, send or deliver information in writing to another person, the requirement is satisfied if the information is provided, sent or delivered, as the case may be, in an electronic record capable of retention by the recipient at the time of receipt. An electronic record is not capable of retention by the recipient if the sender or its information processing system inhibits the ability of the recipient to print or store the electronic record.

(2) If a law other than ORS 84.001 to 84.061 requires a record (i) to be posted or displayed in a certain manner, (ii) to be sent, communicated or transmitted by a specified method, or (iii) to contain information that is formatted in a certain manner, the following rules apply:

(a) The record must be posted or displayed in the manner specified in the other law.

(b) Except as otherwise provided in subsection (4)(b) of this section, the record must be sent, communicated or transmitted by the method specified in the other law.

(c) The record must contain the information formatted in the manner specified in the other law.

(3) If a sender inhibits the ability of a recipient to store or print an electronic record, the electronic record is not enforceable against the recipient.

(4) The requirements of this section may not be varied by agreement, but:

(a) To the extent a law other than ORS 84.001 to 84.061 requires information to be provided, sent or delivered in writing but permits that requirement to be varied by agreement, the requirement under subsection (1) of this section that the information be in the form of an electronic record capable of retention may also be varied by agreement; and

(b) A requirement under a law other than ORS 84.001 to 84.061 to send, communicate or transmit a record by first-class mail, postage prepaid may be varied by agreement to the extent permitted by the other law. [2001 c.535 §8]

84.025 Attribution and effect of electronic record and electronic signature. (1) An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.

(2) The effect of an electronic record or electronic signature attributed to a person under subsection (1) of this section is determined
Chapter 1—Technology on Contracting: Practical and Legal Implications

From the context and surrounding circumstances at the time of its creation, execution or adoption, including the parties’ agreement, if any, and otherwise as provided by law. [2001 c.535 §9]

**84.028 Effect of change or error.** If a change or error in an electronic record occurs in a transmission between parties to a transaction, the following rules apply:

1. If the parties have agreed to use a security procedure to detect changes or errors and one party has conformed to the procedure, but the other party has not, and the nonconforming party would have detected the change or error had that party also conformed, the conforming party may avoid the effect of the changed or erroneous electronic record.

2. In an automated transaction involving an individual, the individual may avoid the effect of an electronic record that resulted from an error made by the individual in dealing with the electronic agent of another person if the electronic agent did not provide an opportunity for the prevention or correction of the error and, at the time the individual learns of the error, the individual:
   a. Promptly notifies the other person of the error and that the individual did not intend to be bound by the electronic record received by the other person;
   b. Takes reasonable steps, including steps that conform to the other person’s reasonable instructions, to return to the other person or, if instructed by the other person, to destroy the consideration received, if any, as a result of the erroneous electronic record; and
   c. Has not used or received any benefit or value from the consideration, if any, received from the other person.

3. If neither subsection (1) nor (2) of this section applies, the change or error has the effect provided by other law, including the law of mistake, and the parties’ contract, if any.

4. Subsections (2) and (3) of this section may not be varied by agreement. [2001 c.535 §10]

**84.031 Notarization and acknowledgment.** If a law requires a signature or record to be notarized, acknowledged, verified or made under oath, the requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the signature or record. [2001 c.535 §11]

**84.034 Retention of electronic records; originals.** (1) If a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record that:

   a. Accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise; and
   b. Remains accessible for later reference.

   2. A requirement to retain a record in accordance with subsection (1) of this section does not apply to any information the sole purpose of which is to enable the record to be sent, communicated or received.

   3. A person may satisfy subsection (1) of this section by using the services of another person if the requirements of subsection (1) of this section are satisfied.

   4. If a law requires a record to be presented or retained in its original form, or provides consequences if the record is not presented or retained in its original form, that law is satisfied by an electronic record retained in accordance with subsection (1) of this section.

   5. If a law requires retention of a check, that requirement is satisfied by retention of an electronic record of the information on the front and back of the check in accordance with subsection (1) of this section.

   6. A record retained as an electronic record in accordance with subsection (1) of this section satisfies a law requiring a person to retain a record for evidentiary, audit or like purposes, unless a law enacted after June 22, 2001, specifically prohibits the use of an electronic record for the specified purpose.

   7. This section does not preclude a governmental agency of this state from specifying additional requirements for the retention of a record subject to the agency’s jurisdiction. [2001 c.535 §12]

**84.037 Admissibility in evidence.** In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form. [2001 c.535 §13]

**84.040 Automated transaction.** In an automated transaction, the following rules apply:

1. A contract may be formed by the interaction of electronic agents of the parties, even if no individual was aware of or reviewed the electronic agents’ actions or the resulting terms and agreements.

2. A contract may be formed by the interaction of an electronic agent and an individual, acting on the individual’s own behalf or for another person, including by an interaction in which the individual performs actions that the individual is free to refuse to perform and that the individual knows or has reason to know will cause the electronic agent to complete the transaction or performance.

3. The terms of a contract are determined by the substantive law applicable to it. [2001 c.535 §14]

**84.043 Time and place of sending and receipt.** (1) Unless otherwise agreed between the sender and the recipient, an electronic record is sent when it:

   a. Is addressed properly or otherwise directed properly to an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record;
84.046 Transferable records. (1) As used in this section, “transferable record” means an electronic record that:

(a) Would be a note under ORS chapter 73 or a document under ORS chapter 77 if the electronic record were in writing; and

(b) The issuer of the electronic record expressly has agreed is a transferable record.

(2) A person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.

(3) A system satisfies subsection (2) of this section, and a person is deemed to have control of a transferable record, if the transferable record is created, stored and assigned in such a manner that:

(a) A single authoritative copy of the transferable record exists that is unique, identifiable and, except as otherwise provided in paragraphs (d), (e) and (f) of this subsection, unalterable;

(b) The authoritative copy identifies the person asserting control as:

(A) The person to which the transferable record was issued; or

(B) If the authoritative copy indicates that the transferable record has been transferred, the person to which the transferable record was most recently transferred;

(c) The authoritative copy is communicated to and maintained by the person asserting control or its designated custodian;

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

(e) Each copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy; and

(f) Any revision of the authoritative copy is readily identifiable as authorized or unauthorized.

(4) Except as otherwise agreed, a person having control of a transferable record is the holder, as defined in ORS 71.2010, of the transferable record and has the same rights and defenses as a holder of an equivalent record or writing under the Uniform Commercial Code, including, if the applicable statutory requirements under ORS 73.0302 (1), 77.5010 or 79.0330 are satisfied, the rights and defenses of a holder in due course, a holder to which a negotiable document of title has been duly negotiated or a purchaser, respectively. Delivery, possession and indorsement are not required to obtain or exercise any of the rights under this subsection.

(5) Except as otherwise agreed, an obligor under a transferable record has the same rights and defenses as an equivalent obligor under equivalent records or writings under the Uniform Commercial Code.

(6) If requested by a person against which enforcement is sought, the person seeking to enforce the transferable record shall provide reasonable proof that the person is in control of the transferable record. Proof may include access to the authoritative copy of the transferable record and related business records sufficient to review the terms of the transferable record and to establish the identity of the person having control of the transferable record. [2001 c.535 §16; 2003 c.14 §32]

84.049 Creation and retention of electronic records by governmental agency; conversion of records into electronic records. (1) A governmental agency of this state shall determine whether, and the extent to which, the governmental agency will create and retain electronic records or convert written records or records that exist in other forms into electronic records.

(2) A person with authority to create or retain custody of a record on behalf of a governmental agency may approve the conversion of the record into an electronic record in accordance with policies the governmental agency adopts. [2001 c.535 §17; 2011 c.39 §3]
Chapter 1—Technology on Contracting: Practical and Legal Implications

84.052 Acceptance and distribution of electronic records by governmental agencies. (1) Except as otherwise provided in ORS 80.034 (6), each governmental agency of this state shall determine whether, and the extent to which, it will send and accept electronic records and electronic signatures to and from other persons and otherwise create, generate, communicate, store, process, use and rely upon electronic records and electronic signatures.

(2) To the extent that a governmental agency uses electronic records and electronic signatures under subsection (1) of this section, the governmental agency, giving due consideration to security, may specify:

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

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

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

(d) Any other required attributes for electronic records that are specified for corresponding nonelectronic records or reasonably necessary under the circumstances.

(3) Except as otherwise provided in ORS 84.034 (6), ORS 84.001 to 84.061 do not require a governmental agency of this state to use or permit the use of electronic records or electronic signatures. [2001 c.535 §18]

84.055 Interoperability. A governmental agency in this state that adopts standards pursuant to ORS 80.052 may encourage and promote consistency and interoperability with similar requirements adopted by other governmental agencies of this state and other states and the federal government and nongovernmental persons interacting with governmental agencies of this state. If appropriate, those standards may specify differing levels of standards from which governmental agencies of this state may choose in implementing the most appropriate standard for a particular application. [2001 c.535 §19]

84.058 Severability clause. If any provision of ORS 80.001 to 80.061 or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions of ORS 80.001 to 80.061 that can be given effect without the invalid provision or application, and to this end the provisions of ORS 80.001 to 80.061 are severable. [2001 c.535 §20]

84.061 Federal electronic signatures law partially superseded. ORS 80.001 to 80.061 constitute the adoption of the Uniform Electronic Transactions Act as approved and recommended for enactment by the National Conference of Commissioners on Uniform State Laws in 1999 and supersede the provisions of section 101 of the federal Electronic Signatures in Global and National Commerce Act (P.L. 106-229) in accordance with section 102(a) of the federal Act. [2001 c.535 §21]

84.063 Rules. A governmental agency may adopt rules necessary to implement the provisions of ORS 80.014 and the amendments to ORS 80.069 by section 3, chapter 39, Oregon Laws 2011. [2011 c.39 §4]

MISCELLANEOUS PROVISIONS

84.064 State Chief Information Officer duties; rules. (1) For purposes of ORS 80.049, 80.052 and 80.055, the State Chief Information Officer shall make determinations and adopt standards for state agencies.

(2) The State Chief Information Officer shall adopt rules to govern state agency use of electronic signatures. The rules must include control processes and procedures to ensure adequate integrity, security and confidentiality for business transactions that state agencies conduct using electronic commerce and to ensure that the transactions can be audited as is necessary for the normal conduct of business.

(3) As used in this section, “state agency” means every state officer and board, commission, department, institution, branch and agency of the state government, the costs of which are paid wholly or in part from funds held in the State Treasury, except:

(a) The Legislative Assembly, the courts, the district attorney for each county and the officers and committees of the Legislative Assembly, the courts and the district attorney; and


84.067 State Archivist duties. Nothing in ORS 80.049 limits or modifies the powers and duties of the State Archivist under ORS 192.005 to 192.170 and 357.805 to 357.895. [2001 c.535 §23]

84.070 Consumer transactions; treatment of oral communications; consent to use of electronic records. (1) As used in this section:

(a) “Consumer” means:

(A) An individual who obtains, through a transaction, products or services that are used primarily for personal, family or household purposes; and

(B) The legal representative of the individual.

(b) “Electronic record,” “information” and “transaction” have the meanings given those terms in ORS 80.004.
Chapter 084

Chapter 1—Technology on Contracting: Practical and Legal Implications

(2) Notwithstanding ORS 84.001 to 84.061, if a statute, rule or other rule of law requires that information relating to a transaction be provided or made available to a consumer in writing, the use of an electronic record to provide or make available, whichever is required, the information satisfies the requirement that the information be in writing if:

(a) The consumer has affirmatively consented to the use of the electronic record and has not withdrawn the consent;

(b) The consumer, before consenting, is provided with a clear and conspicuous statement:

(A) Informing the consumer of:

(i) Any right or option of the consumer to have the record provided or made available on paper or in other nonelectronic form; and

(ii) The right of the consumer to withdraw the consent to have the record provided or made available in an electronic form and of any conditions, consequences, which may include termination of the parties’ relationship, or fees in the event of the withdrawal of the consent;

(B) Informing the consumer of whether the consent applies:

(i) Only to the particular transaction that gave rise to the obligation to provide or make available the record; or

(ii) To identified categories of records that may be provided or made available during the course of the parties’ relationship;

(C) Describing the procedures the consumer must use to withdraw consent as provided in subparagraph (A) of this paragraph and to update information needed to contact the consumer electronically; and

(D) Informing the consumer:

(i) How, after the consent, the consumer may, upon request, obtain a paper copy of an electronic record; and

(ii) Whether any fee will be charged for the paper copy of an electronic record;

(c) The consumer:

(A) Before consenting, is provided with a statement of the hardware and software requirements for access to and retention of the electronic records; and

(B) Consents electronically, or confirms the consent electronically, in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent; and

(d) After the consent of a consumer in accordance with paragraph (a) of this subsection, if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a subsequent electronic record that was the subject of the consent, the person providing the record:

(A) Provides the consumer with a statement of:

(i) The revised hardware and software requirements for access to and retention of the electronic records; and

(ii) The consumer’s right to withdraw consent without imposition of any fees for the withdrawal and without the imposition of any condition or consequence that was not disclosed under paragraph (b)(A) of this subsection; and

(B) Again complies with paragraph (c) of this subsection.

3(a) Nothing in ORS 84.001 to 84.061 affects the content or timing of any disclosure or other record required to be provided or made available to any consumer under any statute, rule or other rule of law.

(b) If a law enacted before October 1, 2000, expressly requires a record to be provided or made available by a specified method that requires verification or acknowledgment of receipt, the record may be provided or made available electronically only if the method used provides verification or acknowledgment of receipt, whichever is required.

(4) The legal effectiveness, validity or enforceability of any contract executed by a consumer may not be denied solely because of the failure to obtain electronic consent or confirmation of consent by that consumer in accordance with subsection (2)(c)(B) of this section.

(5) Withdrawal of consent by a consumer may not affect the legal effectiveness, validity or enforceability of electronic records provided or made available to that consumer in accordance with subsection (2) of this section before implementation of the consumer’s withdrawal of consent. A consumer’s withdrawal of consent is effective within a reasonable period of time after the provider of the record receives the withdrawal. Failure to comply with subsection (2)(d) of this section may, at the election of the consumer, be treated as a withdrawal of consent for purposes of this subsection.

(6) Except as otherwise provided by law, if an insurer can reliably store and reproduce an oral communication or a recording of an oral communication, the oral communication or the recording qualifies as a notice or document delivered by electronic means for the purposes of this section.

(7) Subsections (2) to (6) of this section do not apply to any records that are provided or made available to a consumer who has consented before June 22, 2001, to receive such records in electronic form as permitted by any statute, rule or other rule of law.

(8) Notwithstanding ORS 84.001 to 84.061, if a statute, rule or other rule of law requires that a contract or other record relating to a transaction be provided or made available to a consumer in writing, the legal effectiveness, validity or enforceability of an electronic record of the contract or other record may be denied if the electronic record is not in a form that is capable of being retained and accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record.

(9) Subject to the requirements of subsections (2) and (10)(c) of this section, an electronic record that provides or delivers a notice, offer, disclosure, document, form, correspondence, information or other communication required or permitted under the insurance laws of this state, including but not limited to a notice of a cancellation, termination or nonrenewal of insurance, satisfies the requirement that the notice, offer, disclosure, document, form, correspondence, information or other communication be provided or made available to a consumer in writing. If proof of mailing is sufficient proof of notice, confirmation of electronic delivery of a notice in any form is sufficient proof of notice.

(a) The cancellation or termination of utility services, including water, heat and power;
(b) Default, acceleration, repossession, foreclosure or eviction, or the right to cure, under a credit agreement secured by, or a rental agreement for, a primary residence of an individual;
(c) The cancellation or termination of health insurance or benefits or life insurance benefits, excluding annuities; or
(d) Recall of a product, or material failure of a product, that risks endangering health or safety.
(11) ORS 84.001 to 84.061 do not apply to any document required to accompany any transportation or handling of hazardous materials, pesticides or other toxic or dangerous materials. [2001 c.535 §24; 2005 c.106 §1; 2014 c.34 §1]

84.072 Conditions under which public body may send notice by electronic mail. (1) As used in this section:
(a) “Agreement” has the meaning given that term in ORS 84.004.
(b) “Public body” has the meaning given that term in ORS 174.109.
(2) A public body may send to a person by electronic mail a notice that a law of this state requires the public body to send by regular mail if:
(a) The law does not expressly prohibit or restrict the use of electronic mail as a means by which to deliver the notice;
(b) The person enters into an agreement with the public body in which the person provides the public body with an electronic mail address and affirmatively indicates that the public body may use the electronic mail address as a means for sending to the person a notice required by a law of this state;
(c) The public body, before entering into an agreement under paragraph (b) of this subsection, provides the person with a statement that, in a clear and conspicuous manner, informs the person that:
(A) The public body will use the electronic mail address the person provides as the means by which the public body sends to the person a notice required by a law of this state; and
(B) The person may withdraw the person’s agreement to receive the notice by electronic mail and may instead elect to receive the notice by regular mail;
(d) The person has not withdrawn the agreement the person made under paragraph (b) of this subsection.
(3) A public body, in the statement described in subsection (2)(c) of this section and in each notice the public body sends by electronic mail under this section, shall describe a method by which a person who has agreed under subsection (2)(b) of this section to receive a notice by electronic mail may withdraw the person’s agreement.
(4) A notice sent in accordance with ORS 84.043 (1) and this section to an electronic mail address a person has provided under subsection (2) of this section is presumed to have been received as provided in ORS 84.043 (2). A person may rebut this presumption only by showing that the notice did not enter an information processing system as provided in ORS 84.043 (2)(a) or that the notice was not in the form described in ORS 84.043 (2)(b).
(5)(a) Except as otherwise provided in this section, ORS 84.001 to 84.061 apply to a notice that a public body sends under this section and to an agreement between a public body and a person under this section.
(b) For purposes of this section, a notice that a public body sends by electronic mail is an electronic record as defined in ORS 84.004. [2011 c.242 §1]
Economic Development

- Scientific innovation – discovering new biological, chemical and/or physical principles, compounds, processes and materials
- Technology innovation – applying science and knowledge in new ways to produce machines, mechanisms, and devices with unique functionality
- Product Innovation – combining science and technology in new ways that are useful, enjoyable and/or valuable to customers
- Business Model Innovation – organizing products, services, brands, experiences and value propositions in new ways that are adopted by customers
- Diffusion – spread of awareness of new products or businesses by potential adopters
- Adoption – purchase or use of new innovations by people or organizations
Types of Innovation

- Structured (Corporate) Innovation
- Serendipitous Innovation
- Technology Push Innovation
- Serial Entrepreneurial Innovation

Structured (Corporate) Innovation

Typical innovation process for established corporations

- Market trend analysis
- Technology trend analysis
- Innovation target areas
- Iterative R&D
- New product introduction
- Product Management
Serendipitous Innovation

Typical innovation thought process for random individuals

- *This is bugging me….I wonder if you could…*
- *I wish I had a ….*
- *Somebody should make a ........*

Technology Push Innovation

Typical innovation process for engineers, scientists, and compulsive inventors

- *This new technology could….*
- *If you combined these technologies you could…*
- *You could build one of these out of those…*
- *Let’s build the product…*
- *I wonder if anyone would buy this……*
Serial Entrepreneurial Innovation

Typical innovation thought process for stereotypical serial entrepreneurs

- *This is a hot space... VCs are chasing deals...*
- *The exit multiples are high in that space...*
- *Let’s build a team...*
- *I talked to 20 customer prospects…*
- *Let’s build a minimal viable prototype...*
- *I talked to 50 customer prospects…*
- *Let’s pivot to version 2...*
- *I talked to 50 customer prospects...*
- *Let’s build a product*

Sources of Innovation

- Inventors
- Entrepreneurs
- University researchers
- National lab researchers
- Intrapreneurs
- Skunk works
- R&D departments
University Sponsored Research

- Startups can enhance R&D capacity through collaborations with university researchers and labs
- Universities have world-class researchers and scientific equipment
- The university mission (education and fundamental research) can be misaligned with startup commercialization goals, culture and timelines
- Universities have high overhead fees (e.g. 50%) which can be problematic for startups
- Good university collaborations can solve thorny R&D problems or provide 3rd party validation for startups in gaining confidence of investors and customers

University Licenses

- Startups can be formed or strengthened through licensing of university-developed intellectual property
- Universities license their IP through technology transfer offices
- Universities expect high licensing fees (e.g. 3-5% of revenue) which can be problematic for startups
- Licenses typically have limitation on field of use
- Companies based on university IP tend to be more successful due to higher IP barriers vs. competitors
Sources of Capital

- Public capital
- Private capital
- Customer and Supplier capital
- Philanthropic and Impact capital

Public Capital

- Federal Grant Programs (e.g. DOD, DOE, NIH, USDA)
- Small Business Innovation Research (SBIR) program
- Small Business Technology Transfer (STTR) program
- State grant programs
- City and county grant programs and catalytic investments
- National labs programs (e.g. Small Business Voucher)
- Utility innovation programs (e.g. BPA)
Private Capital

- Friends and Family (and Fools)
- Individual Angels
- Angel networks
- Angel conferences
- Angel funds
- Venture Capital funds
- Crowd funding (e.g. Kickstarter)
- Accredited investor platforms (e.g. Angel List, Propel(X))
- Strategic investors (e.g. Google, GE, Dow)
- Private equity
- Mini-IPOs, Conventional IPOs

Investor Spaces

- IT – computers, software, internet, SaaS, Internet-of-Things
- Mobile – wireless communications, mobile apps
- Social – affinity communities, social media
- Food and Beverage – packaged products, food distribution
- MedTech – medical devices, medical informatics
- FinTech – financial technology, cryptocurrency
- CleanTech – renewable energy, food, water, transportation, green building, circular economy, de-carbonization
- BioTech – pharmaceuticals, genomics, synthetic biology
- HardTech – manufacturing, petrochemical processing, heavy industry, conventional energy
- ImpactTech – poverty alleviation, environmental security, food security, infrastructure resiliency
Investor Stages

- Friends, Family (and Fools) – earliest investors based on confidence in entrepreneurs
- Seed – pre-revenue, prototype, proof-of-concept
- Series A – early revenue, product introduction
- Series B,C,D – manufacturing scale-up, sales scale-up, organization scale-up
- Investment Banking – debt financing for operational growth
- Venture Debt – sidecar to equity financing for high potential startups
- IPO – initial public offering
- Acquisition – purchase of startup by existing entity

Oregon Capital Sources

- Managed Funds – perpetual investment funds
  - Oregon Angel Fund
  - Voyager Capital
  - Seven Peaks Ventures
  - Portland Seed Fund
  - Rogue Venture Partners
  - Cascade Angels
  - W2 Fund
- Investment Conferences – annual investments
  - OEN’s Angel Oregon
  - Willamette Angel Conference
  - Bend Venture Conference
Customer and Supplier Capital

- Good source of capital for startups in some situations
- Provides new market opportunities for suppliers
- Provides new product lines for customers who resell to others
- Can be problematic for startup as it reduces negotiating leverage

Philanthropic and Impact Capital

- Alternative startup capital available from Family Offices, Foundations, Wealth Management Firms, High Net Worth Individuals
- Philanthropic Capital is typically grants - seeking alignment with philanthropic goals and themes
- Impact Capital is typically investments – seeking conventional rates-of-return commensurate with asset class combined with positive social or environmental impact aligned with goals or themes
- Impact Capital is a relatively small but rapidly growing asset class
Support Organizations

- Signature Research Centers (Oregon BEST, ONAMI, OTRADI)
- Small Business Development Centers
- Incubators
- Accelerators
- Entrepreneurship Organizations (e.g. OEN, EO)
- Service Corps of Retired Executives

Investment Structures

- Strategic Partnerships
- Royalties (Revenue Loans)
- Convertible Notes
- Priced Equity
- SAFEs
Key Dimensions of Strategic Partnerships

- Typical structure includes investment by existing corporation in startup, some level of exclusivity, joint development arrangements and joint promotion arrangements
- Alignment between startup product and business unit of corporate investors is key factor
- Joint development agreements couple startup innovation with larger corporate resources
- These partnerships can accelerate products to market due to additive resources
- These partnerships can stifle product commercialization due to corporate bureaucracy and changes of direction

Royalties – Key Terms

Good vehicle if startup can grow organically without raising additional capital from other investors

- What revenue stream is covered – this can be tricky
- Percentage of revenue (e.g. 1 - 5% of revenue)
- Definition of revenue – gross vs. net
- Term
- Total cap – e.g. 2X – 4X of investment amount
- Audits
Convertible Notes – Key Terms

Typical vehicle for early angel investors or to finance bridge capital needs between priced rounds of equity

- Term
- Interest rate
- Discount (if any)
- Warrant kicker (if any)
- Valuation cap (anti-dilution protection)
- Class of shares that the note converts into
- Conversion triggers – e.g. priced round of sufficient size
- Security
- Subordination

Priced Equity – Key Terms

Typical vehicle for venture capital and other institutional investors as company grows

- Price per share
- Pre-money valuation
- Liquidation preference
- Voting rights
- Appointment of a Director
- Anti-dilution
- Mandatory conversion
- Participation rights in future rounds
- Employee stock options
- Accredited investor representation
Simple Agreement for Future Equity (SAFE)

Good vehicle for early investors (e.g. friends, families and individual angels)

- Developed by Y Combinator
- Simple alternative to priced equity or convertible notes
- Low cost instrument with minimal legal fees
- Agreement to buy/sell shares in a future round
- No interest, no maturity, no security
- Valuation cap important to professional investors
- SAFE with cap and other varieties of SAFE also in use

Key Dimensions of Startup Readiness for Engaging Investors

- Innovative product
- Intellectual property protection
- Large market potential (large existing or rapidly growing target market)
- Strong initial product differentiation
- Deep pipeline of potential follow-on products
- Clear and compelling customer value proposition
- Testimonials from lead customers
- Strong team with technical skills, business skills, passion, and tenacious attitude
- Convincing revenue and profit scale-up projections
- Well defined go-to-market strategy
- Credible and viable operational strategy
Deal Dynamics

- Motivations
  - Both investor and entrepreneur balancing fear and greed
  - Entrepreneur can be irrational about “the baby”
  - Investor can be too focused on “winning” vs. the marriage
  - Best deals create economic alignment and collaboration between investor and entrepreneur

- Valuations
  - Very difficult to value pre-revenue companies
  - Even post-revenue companies hard to value in new markets with leading edge technology
  - Best way to establish valuation is benchmarks vs. other analytical methods

- Shotgun marriages
  - Forcing new management into the organization as condition of deal is rarely successful

Lean Canvas

Common tool used for fast-track business planning and iterative business model development
## Market Evaluation

- General market being addressed
- Size and growth characteristics
- Total Available Market (TAM)
- Served Available Market (SAM)
- Current competitors and market shares
- Value chain
- Lead customers
- Key distribution channels
- Importance of customer discovery

## Product Development

- Models – software or physical representations
- Proof-of-concept – demonstrations of viability or efficacy of core technology
- Prototype – commercially relevant rough product
- Minimum Viable Prototype – lowest cost prototype that can be used to get feedback in customer discovery
- Pre-production – engineered product in substantially same form of eventual production-ready product
- Production ready – final product ready for replication in manufacturing operations
Key Attributes of Financial Model

Startups need a pro forma financial model to forecast operations, establish valuation and attract capital

- 5 year forecast with more detail in first 2 years
- Clear definitions of key assumptions that impact the model
- Revenue ramp up based on actual customer interactions
- Cost of Good Sold (COGS) with trend variations related to economies of scale
- Manufacturing costs
- Material costs
- Sales and General Administration costs
- Cash flow forecast
- Cumulative cash flow and positive cash flow crossover

Investor Pitch Deck 1

Startups need a short presentation designed to engender enough interest to get a meeting with investors – typically a 5-10 minute pitch delivered at events

- Focused on “sizzle”
- Focused on product, customer value proposition and market potential
- Simple “story telling” format that can get unfamiliar investors to quickly grasp the essential concepts behind the companies’ products and business model
- Enough financial forecasts to demonstrate that the business can be an attractive investment opportunity
### Investor Pitch Deck 2

Startups need a long presentation designed to guide a meeting with investors – typically a 30-40 minute pitch delivered at investor’s office

- Focused on “sizzle and the steak”
- Covers product, customer value proposition, competitive dynamics, market potential, customer traction, operational plan, management team, financial projections, exit strategy
- Easy to follow but informative format that can help the investor understand the unique characteristics of the product, market, business model, the deal terms, and the potential for strong ROI
- Complete 5 year pro forma financial forecasts will be evaluated, challenged and discussed in some detail

### Legal Needs for Startups

- Corporate entity formation
- Advice and counsel
- Connections and introductions
- Confidentiality agreements
- IP assignment agreements
- Patent filings
- Investment transactions
- Stock option plans
- Distribution agreements
- Purchase agreements
Innovators are Awful Legal Clients

- Innovators are typically technical people with limited business skills
- Non-technical innovators are typically “wheeler-dealers” who want to get services for free or at a discount
- Many innovators have little knowledge of the legal aspects of starting and growing a business
- Most startups operate on a financial shoestring and have little understanding of typical legal fee structures and may have difficulty paying legal bills
- Most startups fail, don’t result in long term clients, and equity compensation becomes nothing but wallpaper

Innovators are Awesome Legal Clients

- Innovators are fascinating people with a compulsion to change the world (and make money in the process)
- Startup companies have a variety of legal needs
- Inexperienced CEOs appreciate the wise counsel of experienced corporate attorneys
- Startups engage in interesting strategic transactions
- Successful startups can grow to become large or medium sized companies with the full gamut of corporate legal needs
- Startups are happy to offer equity to their attorneys in exchange for legal services – this can be highly lucrative if the company succeeds
Where to Find Innovators

- Accelerator programs (e.g. OTBC, Cascadia Cleantech Accelerator)
- Entrepreneurship organizations (e.g. Oregon Entrepreneur’s Network)
- Angel groups
- Meet ups
- Conference panels (e.g. BEST FEST, TechFest NW)
Data Visualization: How Your Expert Can Help You Tell Your Story

Presented by:
Serena Morones, CPA, ASA, ABV, CFE
Jennifer Murphy, CPA, CFE, CFF, ABV
Morones Analytics LLC

Topics We Will Cover

1. Taking Your Case from Produced Data to Data Visualization

2. Case Study: Oregon’s 2013 Big Tobacco Litigation
Chapter 3—Data Visualization: How Your Expert Can Help You Tell Your Story—Presentation Slides

Part I: From Produced Data ➔ Data Visualization

Typical role of financial experts in litigation:
Demonstrate financial damages

- Personal Damages
- Breach of Contract
- Product Liability
- Wage and Hour
- Intellectual Property

May include data visualization via charts and graphs

Part I: From Produced Data ➔ Data Visualization

Can use a chart to help visualize damage conclusion:

![Damage Chart]

Law, Practice, and Policy at the Bleeding Edge—2017 Technology Law Updates
Part I: From Produced Data ➔ Data Visualization

Topic of data visualization, also called Data Analytics:

- the science of drawing insights from sources of raw information…Data analytics techniques can reveal trends and metrics that would otherwise be lost in the mass of information. - Investopedia

- a process of inspecting, cleansing, transforming, and modeling data with the goal of discovering useful information, suggesting conclusions, and supporting decision-making. - Wikipedia

Steps Involved in Data Visualization:

1. Define purpose of analysis – what question(s) are we trying to answer?
2. Identify data source(s)
3. Identify best tool for analyzing the data
4. Tame the data
5. Analyze data under the parameters set
6. Present resulting conclusion visually so that it is easily understandable
Part I: From Produced Data → Data Visualization

1. Define purpose of analysis – what question(s) are we trying to answer?
   - In litigation setting, data visualization can be used to synthesize a large volume of factual evidence to the trier of fact.
   - Most data questions can be answered by presenting:
     - Comparison
     - Composition
     - Distribution
     - Relationship

2. Identify data source(s)
   - Data often resides all over the place in various silos that have different owners.
   - Our clients don’t expect to find themselves involved in litigation – data collection on the front end very likely did not anticipate what we are now using it for.
   - Often need to think creatively to make sure we have captured a complete population of data in an accurate and reliable way.
Part I: From Produced Data ➔ Data Visualization

3. Identify best tool for analyzing the data
   - Database software
     - Excel
     - Access
   - Other specialized software – used in “Big Data” setting in the corporate world, beyond the scope of what we typically need.

4. Tame the data
   - Need to normalize the data so it can be accurately analyzed and quantified.
   - This is the most challenging step of the process.
4. **Tame the data**

- Examples of common data problems that require normalizing
  - Data is unstructured – not organized in any predefined manner and text-heavy
  - Data cells commingle different data points, such as including both text and numerical figures
  - Data errors exist in the data collection
  - Data identifiers are not structured consistently over time: old system/new system; change in staff collecting the data; organic changes

- Must be able to identify and fix – but how?
  - Utilize Excel tools – but can’t rely on them to catch everything
  - Apply knowledge gained outside of data collection
  - The analyst should continually perform reasonableness checks on both the data and the results of analysis
Part I: From Produced Data → Data Visualization

5. Analyze data under the parameters set
   • As with any analysis, need to assure completeness and accuracy of computations in order to reach the correct conclusion.
   • During this step, must continue to be aware of any data inconsistencies that were not caught earlier.

6. Present resulting conclusion visually so that it is easily understandable
   • Simplify, minimize extraneous information.
   • Consider how colors, scale and other visual factors can help make your point – while also being careful not to mislead!
Part II: Case Study: Oregon’s 2013 Big Tobacco Litigation

Case background:
- Big Tobacco Manufacturers (Participating Manufacturers or PMs) are required to make annual payments to States in perpetuity under a settlement agreement.
- Settling States, including Oregon, are obligated to enforce a Qualifying Statute related to the collection of escrow payments from Non-Participating Tobacco Manufacturers (NPMs).
- PMs disputed that they owed the full amount of the 2003 settlement payment, citing Oregon’s failure to diligently enforce its Qualifying Statute.

Our role as Experts:
- Oregon needed to show it diligently enforced its Qualifying Statute.
- We synthesized a large volume of data from various sources to determine the enforcement actions taken by Oregon in 2002-2003, including:
  - Cigarette distributor sales reports
  - State tobacco inspector reports
  - Oregon civil NPM enforcement team detailed timekeeping records
  - NPM certificates of compliance, escrow agreements and deposit records
  - Communications between the Oregon DOJ and distributors
Part II: Case Study: Oregon’s 2013 Big Tobacco Litigation

Impact of Oregon Enforcement: Contacting Distributors

Impact of Oregon Enforcement: Enjoining Non-Compliant NPM Sales
Part II: Case Study: Oregon’s 2013 Big Tobacco Litigation

Impact of Oregon Enforcement: Provided Context to Non-Compliant NPMs - “Bad Actors”

Impact of Oregon Enforcement: Data to Support Level of Effort
Part II: Case Study: Oregon’s 2013 Big Tobacco Litigation

Impact of Oregon Enforcement: Data to Support Level of Effort

Thank you!

Serena Morones CPA, ASA, ABV, CFE
Serena@moronesanalytics.com

Jennifer Murphy CPA, CFE, CFF, ABV
Jennifer@moronesanalytics.com
Chapter 4
Where’s Your Data? Data Privacy and Your Ethical Obligations

Calon Russell
Holland & Knight LLP
Portland, Oregon

Dayna Underhill
Holland & Knight LLP
Portland, Oregon

Contents

Presentation Slides ................................................................. 4–1
Selected Oregon Rules of Professional Conduct .......................... 4–17
RPC 1.1, Competence .............................................................. 4–17
RPC 1.6, Confidentiality of Information ..................................... 4–18
RPC 1.15-1, Safekeeping Property, and 1.15-2, IOLTA Accounts and Trust Account Overdraft Notification ........................................... 4–19
RPC 5.1, Responsibilities of Partners, Managers, and Supervisory Lawyers ......................................................... 4–23
RPC 5.2, Responsibilities of a Subordinate Lawyer ....................... 4–24
RPC 5.3, Responsibilities Regarding Nonlawyer Assistance ........ 4–25

Where’s Your Data?
Privacy, Security, and your Ethical Obligations

Oregon State Bar Technology Law Update
Portland, Oregon
October 5, 2017
Dayna E. Underhill and Calon N. Russell

It Can (and likely will) Happen to You

“I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.”

Former FBI Director Robert S. Mueller, III
RSA Cyber Security Conference
San Francisco, CA
March 1, 2012
It happens to the best of us...

What Do We Do Next and Why?

Holland & Knight
Why do we care?

» Ethical Obligations
  - Competence
  - Confidentiality
  - Safekeeping client property
  - Supervising subordinate lawyers and non-lawyer staff

» Statutory Obligations
  - State and Federal Law (Data Breach Notification, SEC Guidance, IRS Enforcement)

» Remaining Competitive in the Marketplace
  - Engagements
  - Client audits

What does a data breach look like and who is doing it?
What Are the Biggest Threats?

- Insider theft: 14%
- Hacking: 17%
- Accidental exposure or negligence: 42%
- Subcontractor: 27%

---

Hackers
Phishing/Malware

Your personal files are encrypted!

Private key will be destroyed on
9/24/2013
6:02 PM
Time left
54:15:15

Holland & Knight

Mobile Lawyering

Holland & Knight
Data Storage Methods

Cloud Storage Can Create Risk

A look inside one of the data centers operated by 1&1 Internet, which is among the companies with the most web servers.
What are they looking for?

Value

» Access to anything of value. And law firms, large and small, have it all.

- Money Social Security Numbers
- Addresses
- Net Worth
- Commercially Valuable Confidential Information/Trade Secrets
- Litigation Secrets
- Other Information Not Publicly Available
Not a surprise: lawyers must be competent
**Duty of Competence – RPC 1.1**

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

ABA Cmt [8]: Lawyer must “maintain” competence by keeping abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education.

**Duty of Confidentiality – RPC 1.6(c)**

A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.
Oregon Formal Ethics Opinion 2011-188

- **Confidentiality**: lawyer must take reasonable steps to ensure that the storage company will reliably secure client data and keep information confidential.

- May be enough to comply with industry standards.

- As technology advances, the third-party vendor’s protective measures may become less secure or obsolete over time. Lawyer may be required to reevaluate the protective measures.

What Are “Reasonable Efforts”?

Holland & Knight
Do You Need a Zombie House? Consider:

- Sensitivity of the information;
- Is disclosure likely if add’l safeguards not employed;
- Cost of employing add’l safeguards;
- Difficulty of implementing the safeguards; and
- Extent to which safeguards adversely affect the lawyer’s ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

If Not a Zombie House, Then What?

- Use secure networks (access control), where possible
- Use encrypting technology
- Inactivity timer
- Location services
- Remote wipe
- URLs and QRs
- Update your device
- Don’t jailbreak or root
- Terms of Service
- Use strong passwords and change them regularly
Lawyer’s Duties of Supervision

Everyone in the firm shares in the responsibility:

- **RPC 5.1:** Partners, managers and supervisory lawyers
- **RPC 5.2:** Subordinate Lawyers remain responsible even if acting at direction of another
- **RPC 5.3:** Nonlawyers employed, retained, supervised or directed by lawyer

**TRAINING IS KEY**

Clients Can Control Their Data/Engagements

- A client may require the lawyer to implement special security measures
- A client may give informed consent to forgo security measures that would otherwise be required
Talk To Your Clients

• Talk to your client about passwords, mobile devices & shared-access accounts

Mobile / Computer Access – Change Account Passwords

Please think about who has access to your confidential, financial, or otherwise personal information. This type of information can be kept on your smartphones, emails, files, thumb drives, in the cloud and on other electronic storage devices. It is essential that you, and only you, control who has access to this information and that you take steps to secure it from others, including the opposing party and their lawyer.

As a result, I recommend that you change your password on all accounts and devices on which another person may have access, including your smartphone, computer, websites (such as banks and cloud services), and email. You should use two-factor authorization and a strong password.

Everyone is an expert after the fact – be an expert beforehand
Chapter 4—Where’s Your Data? Data Privacy and Your Ethical Obligations

**Be Prepared For a Breach**

Conduct a systems assessment – what do you have, what do you need and where are your holes?

Hire an IT Expert and respect their expertise

Identify a firm IT policy/crisis/document response team
- Include IT, lawyers, staff
- Consider legal & ethical obligations and business objectives

Create polices and conduct training – and TEST!

Evaluate third-party vendors (including the cloud)

Consider cyber-insurance and compare to LPL

**Respond to a Breach Appropriately**

1. Assemble your team
2. Secure your network, investigate and identify compromised data
3. Make necessary notifications
4. Remedy breach / respond to client complaints and consumer issues
5. Follow up including lessons learned
Thank you!

Dayna E. Underhill  
Calon N. Russell  
Holland & Knight LLP  
Phone: 503.243.5891  
Email: Dayna.Underhill@hklaw.com  
Email: Calon.Russell@hklaw.com
RULE 1.1 COMPETENCE

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.
RULE 1.6 CONFIDENTIALITY OF INFORMATION

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

(1) to disclose the intention of the lawyer's client to commit a crime and the information necessary to prevent the crime;

(2) to prevent reasonably certain death or substantial bodily harm;

(3) to secure legal advice about the lawyer's compliance with these Rules;

(4) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client;

(5) to comply with other law, court order, or as permitted by these Rules; or

(6) in connection with the sale of a law practice under Rule 1.17 or to detect and resolve conflicts of interest arising from the lawyer’s change of employment or from changes in the composition or ownership of a firm. In those circumstances, a lawyer may disclose with respect to each affected client the client's identity, the identities of any adverse parties, the nature and extent of the legal services involved, and fee and payment information, but only if the information revealed would not compromise the attorney-client privilege or otherwise prejudice any of the clients. The lawyer or lawyers receiving the information shall have the same responsibilities as the disclosing lawyer to preserve the information regardless of the outcome of the contemplated transaction.

(7) to comply with the terms of a diversion agreement, probation, conditional reinstatement or conditional admission pursuant to BR 2.10, BR 6.2, BR 8.7 or Rule for Admission Rule 6.15. A lawyer serving as a monitor of another lawyer on diversion, probation, conditional reinstatement or conditional admission shall have the same responsibilities as the monitored lawyer to preserve information relating to the representation of the monitored lawyer’s clients, except to the extent reasonably necessary to carry out the monitoring lawyer’s responsibilities under the terms of the diversion, probation, conditional reinstatement or conditional admission and in any proceeding relating thereto.

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.
RULE 1.15-1 SAFEKEEPING PROPERTY

(a) A lawyer shall hold property of clients or third persons that is in a lawyer's possession separate from the lawyer's own property. Funds, including advances for costs and expenses and escrow and other funds held for another, shall be kept in a separate "Lawyer Trust Account" maintained in the jurisdiction where the lawyer's office is situated. Each lawyer trust account shall be an interest bearing account in a financial institution selected by the lawyer or law firm in the exercise of reasonable care. Lawyer trust accounts shall conform to the rules in the jurisdictions in which the accounts are maintained. Other property shall be identified as such and appropriately safeguarded. Complete records of such account funds and other property shall be kept by the lawyer and shall be preserved for a period of five years after termination of the representation.

(b) A lawyer may deposit the lawyer's own funds in a lawyer trust account for the sole purposes of paying bank service charges or meeting minimum balance requirements on that account, but only in amounts necessary for those purposes.

(c) A lawyer shall deposit into a lawyer trust account legal fees and expenses that have been paid in advance, to be withdrawn by the lawyer only as fees are earned or expenses incurred, unless the fee is denominated as “earned on receipt,” “nonrefundable” or similar terms and complies with Rule 1.5(c)(3).

(d) Upon receiving funds or other property in which a client or third person has an interest, a lawyer shall promptly notify the client or third person. Except as stated in this rule or otherwise permitted by law or by agreement with the client, a lawyer shall promptly deliver to the client or third person any funds or other property that the client or third person is entitled to receive and, upon request by the client or third person, shall promptly render a full accounting regarding such property.

(e) When in the course of representation a lawyer is in possession of property in which two or more persons (one of whom may be the lawyer) claim interests, the property shall be kept separate by the lawyer until the dispute is resolved. The lawyer shall promptly distribute all portions of the property as to which the interests are not in dispute.

RULE 1.15-2 IOLTA ACCOUNTS AND TRUST ACCOUNT OVERDRAFT NOTIFICATION

(a) A lawyer trust account for client funds that cannot earn interest in excess of the costs of generating such interest (“net interest”) shall be referred to as an IOLTA (Interest on Lawyer Trust Accounts) account. IOLTA accounts shall be operated in accordance with this rule and with operating regulations and procedures as may be established by the Oregon State Bar with the approval of the Oregon Supreme Court.

(b) All client funds shall be deposited in the lawyer’s or law firm’s IOLTA account unless a particular client’s funds can earn net interest. All interest earned by funds held in the IOLTA account shall be paid to the Oregon Law Foundation as provided in this rule.
(c) Client funds that can earn net interest shall be deposited in an interest bearing trust account for the client’s benefit and the net interest earned by funds in such an account shall be held in trust as property of the client in the same manner as is provided in paragraphs (a) through (d) of Rule 1.15-1 for the principal funds of the client. The interest bearing account shall be either:

1. a separate account for each particular client or client matter; or
2. a pooled lawyer trust account with sub accounting which will provide for computation of interest earned by each client's funds and the payment thereof, net of any bank service charges, to each client.

(d) In determining whether client funds can or cannot earn net interest, the lawyer or law firm shall consider the following factors:

1. the amount of the funds to be deposited;
2. the expected duration of the deposit, including the likelihood of delay in the matter for which the funds are held;
3. the rates of interest at financial institutions where the funds are to be deposited;
4. the cost of establishing and administering a separate interest bearing lawyer trust account for the client’s benefit, including service charges imposed by financial institutions, the cost of the lawyer or law firm's services, and the cost of preparing any tax-related documents to report or account for income accruing to the client’s benefit;
5. the capability of financial institutions, the lawyer or the law firm to calculate and pay income to individual clients; and
6. any other circumstances that affect the ability of the client’s funds to earn a net return for the client.

(e) The lawyer or law firm shall review the IOLTA account at reasonable intervals to determine whether circumstances have changed that require further action with respect to the funds of a particular client.

(f) If a lawyer or law firm determines that a particular client’s funds in an IOLTA account either did or can earn net interest, the lawyer shall transfer the funds into an account specified in paragraph (c) of this rule and request a refund for the lesser of either: any interest earned by the client’s funds and remitted to the Oregon Law Foundation; or the interest the client’s funds would have earned had those funds been placed in an interest bearing account for the benefit of the client at the same bank.

1. The request shall be made in writing to the Oregon Law Foundation within a reasonable period of time after the interest was remitted to the Foundation and shall be accompanied by written verification from the financial institution of the interest amount.
(2) The Oregon Law Foundation will not refund more than the amount of interest it received from the client’s funds in question. The refund shall be remitted to the financial institution for transmittal to the lawyer or law firm, after appropriate accounting and reporting.

(g) No earnings from a lawyer trust account shall be made available to a lawyer or the lawyer’s firm.

(h) A lawyer or law firm may maintain a lawyer trust account only at a financial institution that:

(1) is authorized by state or federal banking laws to transact banking business in the state where the account is maintained;

(2) is insured by the Federal Deposit Insurance Corporation or an analogous federal government agency;

(3) has entered into an agreement with the Oregon Law Foundation:

(i) to remit to the Oregon Law Foundation, at least quarterly, interest earned by the IOLTA account, computed in accordance with the institution’s standard accounting practices, less reasonable service charges, if any; and

(ii) to deliver to the Oregon Law Foundation a report with each remittance showing the name of the lawyer or law firm for whom the remittance is sent, the number of the IOLTA account as assigned by the financial institution, the average daily collected account balance or the balance on which the interest remitted was otherwise computed for each month for which the remittance is made, the rate of interest applied, the period for which the remittance is made, and the amount and description of any service charges deducted during the remittance period; and

(4) has entered into an overdraft notification agreement with the Oregon State Bar requiring the financial institution to report to the Oregon State Bar Disciplinary Counsel when any properly payable instrument is presented against such account containing insufficient funds, whether or not the instrument is honored.

(i) Overdraft notification agreements with financial institutions shall require that the following information be provided in writing to Disciplinary Counsel within ten banking days of the date the item was returned unpaid:

(1) the identity of the financial institution;

(2) the identity of the lawyer or law firm;

(3) the account number; and

(4) either (i) the amount of the overdraft and the date it was created; or (ii) the amount of the returned instrument and the date it was returned.
(j) Agreements between financial institutions and the Oregon State Bar or the Oregon Law Foundation shall apply to all branches of the financial institution. Such agreements shall not be canceled except upon a thirty-day notice in writing to OSB Disciplinary Counsel in the case of a trust account overdraft notification agreement or to the Oregon Law Foundation in the case of an IOLTA agreement.

(k) Nothing in this rule shall preclude financial institutions which participate in any trust account overdraft notification program from charging lawyers or law firms for the reasonable costs incurred by the financial institutions in participating in such program.

(l) Every lawyer who receives notification from a financial institution that any instrument presented against his or her lawyer trust account was presented against insufficient funds, whether or not the instrument was honored, shall promptly notify Disciplinary Counsel in writing of the same information required by paragraph (i). The lawyer shall include a full explanation of the cause of the overdraft.

(m) For the purposes of paragraph (h)(3), “service charges” are limited to the institution’s following customary check and deposit processing charges: monthly maintenance fees, per item check charges, items deposited charges and per deposit charges. Any other fees or transactions costs are not “service charges” for purposes of paragraph (h)(3) and must be paid by the lawyer or law firm.
RULE 5.1 RESPONSIBILITIES OF PARTNERS, MANAGERS, AND SUPERVISORY LAWYERS

A lawyer shall be responsible for another lawyer's violation of these Rules of Professional Conduct if:

(a) the lawyer orders or, with knowledge of the specific conduct, ratifies the conduct involved; or

(b) the lawyer is a partner or has comparable managerial authority in the law firm in which the other lawyer practices, or has direct supervisory authority over the other lawyer, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.
RULE 5.2 RESPONSIBILITIES OF A SUBORDINATE LAWYER

(a) A lawyer is bound by the Rules of Professional Conduct notwithstanding that the lawyer acted at the direction of another person.

(b) A subordinate lawyer does not violate the Rules of Professional Conduct if that lawyer acts in accordance with a supervisory lawyer's reasonable resolution of an arguable question of professional duty.
RULE 5.3 RESPONSIBILITIES REGARDING NONLAWYER ASSISTANCE

With respect to a nonlawyer employed or retained, supervised or directed by a lawyer:

(a) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and

(b) except as provided by Rule 8.4(b), a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:

(1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or

(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.
FORMAL OPINION NO 2011-188
[REVISED 2015]

Information Relating to the Representation of a Client:
Third-Party Electronic Storage of Client Materials

Facts:

Law Firm contracts with third-party vendor to store client files and
documents online on remote server so that Lawyer and/or Client could
access the documents over the Internet from any remote location.

Question:

May Lawyer do so?

Conclusion:

Yes, qualified.

Discussion:

With certain limited exceptions, the Oregon Rules of Professional
Conduct require a lawyer to keep client information confidential. See
Oregon RPC 1.6.¹ In addition, Oregon RPC 5.3 provides:

¹ Oregon RPC 1.6 provides:

(a) A lawyer shall not reveal information relating to the
representation of a client unless the client gives informed consent, the
disclosure is impliedly authorized in order to carry out the repre-
sentation or the disclosure is permitted by paragraph (b).

(b) A lawyer may reveal information relating to the repre-
sentation of a client to the extent the lawyer reasonably believes neces-
sary:

(1) to disclose the intention of the lawyer’s client to
commit a crime and the information necessary to prevent the crime;

(2) to prevent reasonably certain death or substantial bodily
harm;

(3) to secure legal advice about the lawyer’s compliance
with these Rules;
With respect to a nonlawyer employed or retained, supervised or directed by a lawyer:

(4) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer’s representation of the client;

(5) to comply with other law, court order, or as permitted by these Rules; or

(6) in connection with the sale of a law practice under Rule 1.17 or to detect and resolve conflicts of interest arising from the lawyer’s change of employment or from changes in the composition or ownership of a firm. In those circumstances, a lawyer may disclose with respect to each affected client the client’s identity, the identities of any adverse parties, the nature and extent of the legal services involved, and fee and payment information, but only if the information revealed would not compromise the attorney-client privilege or otherwise prejudice any of the clients. The lawyer or lawyers receiving the information shall have the same responsibilities as the disclosing lawyer to preserve the information regardless of the outcome of the contemplated transaction.

(7) to comply with the terms of a diversion agreement, probation, conditional reinstatement or conditional admission pursuant to BR 2.10, BR 6.2, BR 8.7 or Rule for Admission Rule 6.15. A lawyer serving as a monitor of another lawyer on diversion, probation, conditional reinstatement or conditional admission shall have the same responsibilities as the monitored lawyer to preserve information relating to the representation of the monitored lawyer’s clients, except to the extent reasonably necessary to carry out the monitoring lawyer’s responsibilities under the terms of the diversion, probation, conditional reinstatement or conditional admission and in any proceeding relating thereto.

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.
Lawyer may store client materials on a third-party server as long as Lawyer complies with the duties of competence and confidentiality to reasonably keep the client’s information secure within a given situation.\(^2\) To do so, the lawyer must take reasonable steps to ensure that the storage company will reliably secure client data and keep information confidential.\(^3\) \textit{See} Oregon RPC 1.6(c). Under certain circumstances, this may be satisfied through a third-party vendor’s compliance with industry standards.

\(^2\) Some call the factual scenario presented above “cloud computing.” \textit{See} Richard Acello, \textit{Get Your Head in the Cloud}, 96-Apr ABA Journal 28, 28–29 (April 2010) (providing that “cloud computing” is a “sophisticated form of remote electronic data storage on the Internet” and “[u]nlike traditional methods that maintain data on a computer or server at a law office or other place of business, data stored ‘in the cloud’ is kept on large servers located elsewhere and maintained by a vendor”).

\(^3\) In 2014, leaked documents indicated that several intelligence agencies had the capability of obtaining electronic data and monitoring electronic communications between, among others, attorneys and clients through highly sophisticated methods beyond the capabilities of the general public. Oregon RPC 1.6(c) would not require an attorney to protect a client’s data against this type of advanced interception, as it only requires an attorney to take reasonable steps to secure client data. Nevertheless, an attorney may want to take additional security precautions if he or she handles clients or matters that involve national security interests.
standards relating to confidentiality and security, provided that those industry standards meet the minimum requirements imposed on the Lawyer by the Oregon Rules of Professional Conduct. This may include, among other things, ensuring the service agreement requires the vendor to preserve the confidentiality and security of the materials. It may also require that vendor notify Lawyer of any nonauthorized third-party access to the materials. Lawyer should also investigate how the vendor backs up and stores its data and metadata to ensure compliance with the Lawyer’s duties.4

Although the third-party vendor may have reasonable protective measures in place to safeguard the client materials, the reasonableness of the steps taken will be measured against the technology “available at the time to secure data against unintentional disclosure.”5 As technology advances, the third-party vendor’s protective measures may become less secure or obsolete over time.6 Accordingly, Lawyer may be required to

---

4 See OSB Formal Ethics Op No 2005-141 (rev 2015), which provides:

As long as Law Firm makes reasonable efforts to ensure that the recycling company’s conduct is compatible with Law Firm’s obligation to protect client information, the proposed conduct is permissible. Reasonable efforts include, at least, instructing the recycling company about Law Firm’s duties pursuant to Oregon RPC 1.6 and obtaining its agreement to treat all materials appropriately.

See also OSB Formal Ethics Op No 2005-129 (rev 2014); OSB Formal Ethics Op No 2005-44.

5 See New Jersey Ethics Op No 701 (discussing electronic storage and access to files).

6 See Arizona Ethics Op No 09-04 (discussing confidentiality, maintaining client files, electronic storage, and the Internet).
reevaluate the protective measures used by the third-party vendor to safeguard the client materials.\(^7\)

**Approved by Board of Governors, April 2015.**

---

\(^7\) A lawyer’s obligation in the event of a breach of security of confidential materials is outside the scope of this opinion.

**COMMENT:** For additional information on this general topic and other related subjects, see *The Ethical Oregon Lawyer* § 6.2-1 (confidentiality), § 13.3-3 (employment of nonlawyers), § 16.4-5(c) (third-party electronic storage of client materials) (OSB Legal Pubs 2015); and *Restatement (Third) of the Law Governing Lawyers* §§ 59–60 (2000) (supplemented periodically).