Creating Enforceable Electronic Transactions

Thomas J. Smedinghoff
Baker & McKenzie

What is required to do transactions on the Internet? In a commercial environment, parties enter into an endless variety of different types of transactions. These include contracts governing the purchase and sale of goods, lease agreements, negotiable instruments, agreements for the creation of security interests, loan agreements and promissory notes, filings with government agencies, assignments of rights or title, license agreements, insurance contracts, proxy agreements, and the like. As commerce moves to the Internet, there is an ever-increasing desire to conduct these transactions in that electronic medium. This chapter will address the legal issues raised by the process of entering into a transaction using electronic means. It will focus primarily on U.S. law, although the issues are primarily the same worldwide.

Like all transactions, electronic transactions involve documents, usually referred to as “records” or “electronic records,” and signatures, usually referred to as “electronic signatures” that are created, communicated, and stored in electronic form. They may be created through the manual efforts of an individual (e.g., typing an e-mail message), via the automated processing of computers (e.g., via electronic agents), or via a combination of human interaction with a computer agent (e.g., when an individual accesses a web site and enters into a purchase agreement). They are communicated via an electronic medium, such as the Internet or a private value-added network, and they are typically stored on a computer-readable medium, such as a disk, tape, CD-ROM, or DVD-ROM. Typically, evidence of electronic transactions never exists on
paper, unless there is a need to provide a copy or to introduce evidence to a court or other fact finder.

1. Key Issues for Electronic Transactions

For anyone desiring to conduct their business transactions online, the goal, of course, is to ensure that each electronic transaction is legally valid, binding, and enforceable. This requires consideration of three fundamental legal issues:

- **Is the transaction enforceable in electronic form?** That is, under applicable law, can the transaction in issue (e.g., contract, security interest, negotiable instrument, etc.) be done in electronic form, and if so, has the transaction been properly effected so as to ensure that it will be legally enforceable?

- **Do the parties trust the message?** Are the parties to the transaction sufficiently comfortable with the authenticity and integrity of the electronic documents comprising the transaction such that they are willing to ship their products, transfer funds, provide services, change their position, or otherwise act in reliance on electronic records communicated over the Internet, especially when asked to do so in a real-time environment? In many respects, this boils down to the question of whether the details of the transaction are ultimately provable and enforceable in a court of law.\(^5\)

- **What rules govern doing the transaction in electronic form?** What are the rules that govern the conduct of the parties with respect to doing the transaction in electronic form, including rules regarding the time a message is sent, the time the message is received, the place the message is sent from and received at, incorporation by reference, the creation and recordkeeping relating to the transaction, etc.? Will rules applicable to paper-based transactions also be applicable to the same transactions in electronic form, or do new and/or different rules apply in an electronic environment?

This chapter will examine these three fundamental questions as they apply to transactions in the online environment.

2. Is the Transaction Enforceable in Electronic Form?

For every business, commercial, and governmental transaction – whether it be a contract for the sale or lease of goods, the license of intellectual property, granting of a security interest in collateral, filing a document required by statute or regulation, or any other transaction -- we must address the basic question of whether this particular transaction will be legally valid and enforceable if done in electronic form. To answer this question, we must focus on the requirements for enforceability that arise solely because of the electronic nature of the transaction. This assumes, of course, that the

---

\(^5\) There are, of course, other issues relating to trust, including the creditworthiness of the other party, confidence in the other party’s ability to perform, etc. However, these issues remain the same regardless of whether the transaction takes place via paper or electronically, and are not addressed here. Here, we focus on trust as it relates to the authenticity and integrity of the electronic records that form the basis of the transaction.
fundamental legal elements required for the specified transaction are otherwise present and satisfied. For example, if the transaction involves entering into a contract, we assume that the basic requirements of a contract – e.g., offer, acceptance, consideration, etc. – are present, and focus only on the additional requirements for enforceability that arise because of the electronic nature of the transaction.

### 2.1 What Law Governs Enforceability?

The enforceability of electronic transactions has been the subject of extensive legislative efforts. All 50 states, the U.S. Federal Government, and the governments of at least 55 other countries have enacted or are currently considering some form of legislation governing the enforceability and conduct of electronic transactions.\(^6\) In the U.S., the enforceability of electronic transactions is primarily governed by the Electronic Signatures in Global and National Commerce Act (E-SIGN)\(^2\) that was enacted by Congress in 2000 and largely preempts inconsistent state law, and the Uniform Electronic Transactions Act ("UETA"),\(^8\) which was finalized by the National Conference of Commissioners on Uniform State Laws ("NCCUSL") in 1999 and has now been adopted by 37 states.\(^9\) Relatedly, the European Union has adopted a Directive on a Common Framework for Electronic Signatures for the European Union in 1999;\(^10\) and the United Nations Commission on International Trade Law ("UNCITRAL") Working Group on Electronic Commerce\(^11\) completed work on its Model Law on Electronic Commerce\(^12\) in 1996, and is expected to finalize and approve its Model Law on Electronic Signatures in 2001.\(^13\)

Based on the current legislation being proposed and enacted in the U.S. and internationally relating to electronic transactions, the question of enforceability requires that the parties focus on the following questions:

---


\(^7\) Electronic Signatures in Global and National Commerce Act (E-SIGN), S. 761, P.L. 106-229, 15 U.S.C. 7001 et. seq., signed by President Clinton on June 30, 2000 and effective October 1, 2000

\(^8\) Uniform Electronic Transactions Act (UETA), approved by the National Conference of Commissioners on Uniform State Laws (NCCUSL) on July 23, 1999. A copy of this Act is available at www.law.upenn.edu/bll/ulc/frac99/1999os/ueta99.htm. As of July 2001, 37 states had enacted the UETA. For an updated list of those states that have enacted the UETA, see www.bakernet.com/ecommerce/uetacomp.htm.

\(^9\) See www.bakernet.com/ecommerce/uetacomp.htm for an up-to-date list of states that have adopted UETA.


\(^11\) UNCITRAL is the body within the United Nations primarily charged with oversight of international commercial law. It was created in 1966 by General Assembly Resolution 2205 (XXI) in order to enable the United Nations to play a more active role in reducing or removing legal obstacles to the flow of international trade. A list of its completed projects and their current status may be found at UNCITRAL’s home page www.un.or.at/uncital.” Amelia H. Boss, Electronic Commerce and the Symbiotic Relationship Between International and Domestic Law Reform, 72 TULANE L. REV. 1932, n.3 (1998).


• **Authorization.** Does the law allow this type of transaction to be conducted in electronic form?

• **Consent.** Have the parties consented to conduct this transaction in electronic form?

• **Signature.** Have the signature formalities required for this transaction (where applicable) been satisfied with a legally-recognized form of electronic signature?

• **Record Accessibility.** Are copies of the records comprising the transaction available to all parties?

• **Recordkeeping.** Will the electronic records of this transaction satisfy applicable legal requirements?

We will briefly address each of these issues.

### 2.2 Authorization

As a result of E-SIGN and UETA, most transactions in the U.S. can now be done in electronic form. The Federal E-SIGN Act essentially authorizes “any transaction in or affecting interstate or foreign commerce” to be conducted in electronic form using electronic signatures.\(^{15}\) It effectively sweeps away a myriad of inconsistent state and federal law requirements for paper and ink documents and signatures, as well as multiple inconsistent state requirements for enforceable electronic transactions,\(^ {16}\) and permits electronic commerce to proceed on a substantially uniform legal basis nationwide. E-SIGN preempts all inconsistent state legislation, other than state enactments of UETA in the form promulgated by NCCUSL. UETA achieves essentially the same result, authorizing the use of “electronic records and electronic signatures relating to a transaction.”\(^ {17}\)

The “authorization” provided by E-SIGN and UETA is stated in the negative. E-SIGN provides that, notwithstanding any other rule of law, “a signature, 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 it is in electronic form.”\(^ {18}\) Likewise, UETA provides that “a record or signature may not be denied legal effect or

---

\(^{14}\) The term “transaction” is defined in the E-SIGN Act as “an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons, including any of the following types of conduct – (A) the sale, lease, exchange, licensing, or other disposition of (i) personal property, including goods and intangibles, (ii) services, and (iii) any combination thereof; and (B) the sale, lease, exchange, or other disposition of any interest in real property, or any combination thereof.” E-SIGN Section 106(13).

\(^{15}\) E-SIGN Section 101(a).


\(^{17}\) UETA Section 3(a). UETA Section 2(16) defines “Transaction” as “an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.”

\(^{18}\) E-SIGN Section 101(a).
enforceability solely because it is in electronic form.\textsuperscript{19} UETA also goes somewhat further, affirmatively stating that “if a law requires a record to be in writing, an electronic record satisfies the law”, and “if a law requires a signature, an electronic signature satisfies the law.”\textsuperscript{20} Nonetheless, the effect of these statutes is important (at least for covered transactions) because it prohibits a holding that such transactions are unenforceable solely because of the fact that they are conducted in electronic form.

While both of these Acts cover electronic records and signatures that are used in a business, commercial (including consumer), or governmental transaction, their operative provisions relate to requirements for writings and signatures under other laws. But they do not affect all other laws that require writings and signatures. Both E-SIGN and UETA contain a variety of exceptions to the scope of transactions they authorize in electronic form.

E-SIGN does not apply to transactions governed by the following laws or to the electronic use of the following documents:

- all articles of the UCC, other than Sections 1-107 and 1-206, and Articles 2 and 2A;
- laws governing the creation and execution of wills, codicils, or testamentary trusts;
- laws governing family law matters such as adoption or divorce;
- court orders or notices and other official court documents required to be executed in connection with court proceedings;
- notices of cancellation or termination of utility services,
- notices of default, acceleration, repossession, foreclosure, or eviction, or of the right to cure, under a mortgage or rental agreement for the primary residence of an individual;
- notices of the cancellation of health insurance or benefits or life insurance benefits (excluding annuities);
- notices of the recall of a product, or material failure of a product that risks endangering health or safety; and
- any document required to accompany the transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.\textsuperscript{21}

Likewise, UETA does not apply to transactions governed by the following laws:

- all articles of the UCC, other than Sections 1-107 and 1-206, and Articles 2 and 2A;
- laws governing the creation and execution of wills, codicils, or testamentary trusts;

\textsuperscript{19} UETA Section 7(a).
\textsuperscript{20} UETA Sections 7(c) and 7(d).
\textsuperscript{21} E-SIGN Section 103.
• the Uniform Computer Information Transactions Act (UCITA)
• other laws specified by the enacting state.\textsuperscript{22}

It is also worth noting, however, that neither E-SIGN nor UETA prohibit conducting any of the transactions excluded from their scope in electronic form. Rather, the enforceability of those types of transactions is left to other law, and is are unaffected by this Act.

2.3 Consent

(a) Requirements for All Transactions

As a general matter, both E-SIGN and UETA make clear that a party to a transaction cannot be \textit{required} to conduct that transaction in electronic form.\textsuperscript{23} This preserves the right of a party\textsuperscript{24} to refuse to enter into any transaction in electronic form. Thus, the parties to a transaction retain the right to establish their own requirements regarding the method of communication they will accept.

UETA goes even further, however, and provides that the benefits of the statute will not apply unless the parties have \textit{agreed} to conduct transactions by electronic means.\textsuperscript{25} In other words, UETA is intended as a voluntary (i.e., opt-in) statute that preserves the greatest possible party autonomy to refuse electronic transactions. Whether the parties have agreed to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties conduct,\textsuperscript{26} and may be either express or implied. This requirement can certainly be satisfied with absolute certainty by obtaining an express agreement to do business electronically before relying on electronic transactions,\textsuperscript{27} but agreement can be implied or inferred as well. Thus, for example, if one party sets up a web site that is capable of accepting electronic communications, and another party goes to that web site and enters into a transaction with the first party, it can arguably be inferred that both have impliedly agreed to conduct their transaction in electronic form.

\begin{footnotesize}
\textsuperscript{22} UETA Section 3(b).
\textsuperscript{23} E-SIGN Section 101(b)(2) (“This title does not . . . 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”); UETA Sections 5(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”) and 5(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.”)
\textsuperscript{24} Other than governmental agencies. See E-SIGN Section 101(b)(2).
\textsuperscript{25} UETA Section 5(b). E-SIGN also has consent provisions, but they are limited to a consent to receive records in electronic form in consumer transactions where a rule of law requires that information relating to the transaction be provided or made available to the consumer in writing. See E-SIGN Section 101(c), discussed in part 2(b) below.
\textsuperscript{26} UETA Section 5(b), and comment 3.
\textsuperscript{27} Some states however, require such consent to be in electronic form (see, e.g., California).
\end{footnotesize}
It is unclear how this consent requirement will work in practice. However, it is important to note that UETA also provides that, notwithstanding the fact that a party has given consent to conduct one transaction by electronic means, it may refuse to conduct other transactions by electronic means. Moreover, this provision requiring consent may not be waived by agreement.\textsuperscript{28} This, of course, can have significant implications for a long-term business relationship involving multiple transactions. Presumably either party has the right, at any time, to refuse to continue to conduct future transactions in electronic form, and to require the other party to revert to a paper-based model.

Statutory provisions requiring consent of the parties before electronic transactions will be considered enforceable, as well as statutory provisions making clear that the parties cannot be required to engage in electronic transactions, suggest the advisability of including a provision within the applicable electronic contract whereby each party authorizes and consents to doing the transaction in electronic form.

(b) Requirements for Consumer Transactions

In some cases, special rules have been adopted for consumers entering into online transactions. Specifically, E-SIGN contains an extensive consumer disclosure and consent provision that applies whenever a statute, regulation, or other rule of law requires that information relating to a transaction be provided or made available to a consumer in writing.\textsuperscript{29} In such a case, the use of an electronic record to provide the relevant information to a consumer is acceptable only if the consumer affirmatively consents to the use of an electronic record in lieu of a paper record, and provides such consent electronically, and in a manner that reasonably demonstrates that he can access the electronic information in the form that will be used.\textsuperscript{30}

Prior to consenting, the consumer must be provided with a clear and conspicuous notice that does the following:

- Informs the consumer of his/her option to have the record provided on paper;
- Informs the consumer of his/her option to withdraw such consent;
- Informs the consumer of the conditions, consequences, and fees of withdrawing such consent;
- Informs the consumer of whether the consent applies only to the particular transaction giving rise to the obligation to provide the information, or to identified categories of records that may be made available during the course of the parties’ relationship;
- Describes the procedures the consumer must use to withdraw consent;
- Describes the procedures the consumer must use to update information needed to contact the consumer electronically;
- Informs the consumer how, after consent, he/she may obtain a paper copy of the electronic record, and the fee therefore; and

\textsuperscript{28} UETA Section 5(c).
\textsuperscript{29} E-SIGN Section 101(c).
\textsuperscript{30} E-SIGN Section 101(c)(1)(A) and 101(c)(1)(ii)
Informs the consumer of the hardware and software requirements for access and retention of the electronic records.\textsuperscript{31}

In addition to providing the consumer with the above notices, the contracting business must obtain the consumer’s consent to receive the information electronically rather than on paper, and must also ensure that the consumer can actually receive and access the information in the electronic form in which it will be delivered. To this end, E-SIGN requires that the consumer’s consent must be given or confirmed in a manner that reasonably demonstrates that the consumer can access the information in the electronic form that will be used.\textsuperscript{32} It is not clear from the statute whether this obligation is met if the consumer merely states in an electronic message that he or she can access the electronic records in the specified formats, or otherwise acknowledges or responds affirmatively to an electronic query that asks whether the consumer can access the electronic record. Read literally, the statute requires that the consumer consent in a manner that “reasonably demonstrates” that he or she can actually access the electronic record in the relevant format.

2.4 Signature

Perhaps the biggest issue regarding the enforceability of electronic transactions has been the satisfaction of applicable legal formalities. Specifically, in many cases, the law requires that a transaction be both documented in “writing,”\textsuperscript{33} and “signed” by the person who is sought to be held bound, in order for that agreement to be enforceable. The Statute of Frauds is, of course, the best example of such a law.\textsuperscript{34} In addition, thousands of other federal, state, and local statutes and regulations also require a variety of other types of transactions to be documented by a writing and a signature. In Illinois, for example, over 3,000 statutory sections contain such

\textsuperscript{31} E-SIGN Section 101(c)(1)(B)
\textsuperscript{32} E-SIGN, § 101(c)(1)(C)(ii).
\textsuperscript{33} Requirements that agreements be “in writing” serve a variety of purposes. These include: (1) providing tangible evidence of the existence and nature of the intent of the parties to bind themselves; (2) alerting parties to the consequences of entering into a contract; (3) providing a document that is legible to all, including strangers to the transaction; (4) providing a permanent record of the transaction that remains unaltered over time; (5) allowing the reproduction of a document so that each party can have a copy of the same; (6) allowing for the authentication of the data by means of a signature; (7) providing a document that is in a form acceptable to public authorities and courts; (8) finalizing the intent of the author of the writing and providing a record of that intent; (9) allowing easy storage of data in tangible form; (10) facilitating control and subsequent audit for accounting, tax, or regulatory purposes; and (11) bringing legal rights and obligations into existence in those cases where a “writing” is required for validity purposes. See United Nations, UNCTRAL Model Law on Electronic Commerce with Guide to Enactment 1996, at par. 48, available at www.un.or.at/unctral/english/texts/electcom/ml-ec.htm, and Illinois Commission on Electronic Commerce and Crime, Final Report of the Commission on Electronic Commerce and Crime (May 26, 1998) available at www.bakernet.com/ecommerce.

\textsuperscript{34} For the Statute of Frauds and contracts involving the sale of goods, see U.C.C. § 2-201(1) (1998); see also U.C.C. § 1-206 (1998) (limited enforcement of unsigned, unwritten contracts for the sale of securities for $5,000 or more). See RESTATEMENT (SECOND) OF CONTRACTS § 110 statutory note, at 284-85 (1982) for a state-by-state listing of state statutes of frauds.
requirements. Likewise, Georgia has over 5,500, and Ohio has over 8,000, of such statutory sections. 35

Statutes and regulations that require transactions to be “in writing” and “signed” have generally been perceived to constitute barriers to e-commerce – barriers that must be removed if e-commerce is to flourish. The concern is that an electronic record might not satisfy legal writing requirements, and an electronic signature might not satisfy legal signature requirements. In other words, there was a concern that writing and signature requirements are satisfied only by ink on paper.

In the U.S., that concern has been largely removed by the enactment of the Federal E-SIGN legislation and the Uniform Electronic Transactions Act (UETA). However, that does not end the inquiry. Rather, it is only the beginning.

2.4.1 Why Do You Sign Electronic Documents?

To understand the importance of a signature to an electronic transaction, it is important to consider why a signature might be necessary. Essentially, there are four reasons why an electronic signature might be appropriate for use in connection with an electronic transaction. They can be summarized as follows:

1. **Expression of Intent** – First and foremost, we sign documents to evidence our intent to authenticate the document. The nature of the signer’s intent will vary with the transaction, and in most cases can be determined only by looking at the context in which the signature was made. A signature may, for example, signify an intent to be bound to the terms of the contract, the approval of a subordinate’s request for funding of a project, confirmation that a signer has read and reviewed the contents of a memo, an indication that the signer was the author of a document, or merely that the contents of a document have been shown to the signer and that he or she has had an opportunity to review them.

2. **Legal Requirement** – Second, we sign documents because there is some law or regulation that requires the presence of a signature before the document will be considered legally effective. The statute of frauds (which requires contracts for the sale of goods in excess of $500 to be “signed”) is, of course, the best example of such a law. In addition, however, thousands of other federal, state, and local statutes and regulations also require certain types of transactions to be documented by a writing and a signature.

3. **Identity** – With paper transactions, signatures are sometimes used to identify the person agreeing to be bound by the document, although this is not normally true (e.g., you sign a check to authenticate it, but not necessarily to identify yourself, since your name is typically printed on the check). In the electronic environment, however, where the parties are remote and often not otherwise known to each other, a signature frequently serves the purpose of identifying the signer.

4. **Integrity** – A signature can also be used to ensure document integrity – that is, to ensure that the document has not been altered since it was signed. It is for this reason, for example, that parties to a multi-page contract will sometimes initial each page of the contract. However, on a 10-page paper document, a signature on page 10 does not verify the integrity of the first 9 pages. In the electronic environment, by contrast, certain types of signatures (e.g., digital signatures) can play an important role in verifying the integrity of the entire document.

For electronic transactions, these secondary signature functions of identity and integrity can be key. When transactions are automated, and conducted over significant distances using easily altered digital technology, the need for a way to ensure the identity of the sender and the integrity of the document becomes pivotal. Thus, electronic signatures are often used even when not otherwise required by law.

Unlike the world of paper-based commerce, where the requirement of a signed writing most frequently serves the function of showing that an already identified person made a particular promise, in the e-commerce world, a requirement of a signed electronic message serves not only this function, but the more fundamental function of identifying the person making the promise contained in the message in the first place. This additional function is often critical in e-commerce because there are few other methods of establishing the source of an electronic message.38

### 2.4.2 What Is an Electronic Signature, and How Can You Sign an Electronic Record?

Traditionally, a signature is any *symbol* that is made with the *intent* to sign a document. Thus, for example, the definition of “signed” in the Uniform Commercial Code includes “any *symbol*” so long as it is “executed or adopted by a party with present *intention* to authenticate a writing.”37 The primary focus is on the “intention to authenticate” a document, which distinguishes a signature from an autograph.

Both E-SIGN and UETA take a similar approach with respect to the concept of an electronic signature. Generally, to be enforceable under U.S. law, an electronic signature must possess three elements:

1. a sound, symbol, or process,
2. attached to or logically associated with an electronic record, and
3. made with the intent to sign the electronic record.38

Electronic signatures that meet these requirements are considered legally enforceable as substitutes for handwritten signatures for most transactions in the U.S.39

---

37 U.C.C. Article 1, § 1-201(39) (1999).
38 E-SIGN Section 106(5) and UETA Section 2(8) (definitions of “electronic signature”).
39 See UETA Sections 2(8) and 7(d) and E-SIGN Sections 101(a) and 106(5).
The foregoing definition of electronic signature is a generic, technology-neutral definition, that recognizes that there are many different methods by which one can “sign” an electronic record. In all cases, electronic signatures are represented digitally (i.e., as a series of ones and zeroes), but they can take many forms, and can be created by many different technologies. Examples of electronic signatures include:

- A name typed at the end of an e-mail message by the sender;
- A digitized image of a handwritten signature that is attached to an electronic document (sometimes created via a biometrics-based technology called signature dynamics[^40]);
- A secret code, password, or PIN to identify the sender to the recipient (such as that used with ATM cards and credit cards);
- A unique biometrics-based identifier, such as a fingerprint, voice print, or a retinal scan;
- A mouse click (such as on an “I accept” button);[^41]
- A sound (e.g., the sound created by pressing “9” on your phone to agree); and
- A “digital signature” (created through the use of public key cryptography).

Note that a digital signature[^42] is simply a term for one technology-specific type of electronic signature. It involves the use of public key cryptography[^43] to “sign” an electronic record.^[44]

[^40]: Under the California Digital Signature Regulations, “Signature Dynamics’ means measuring the way a person writes his or her signature by hand on a flat surface and binding the measurements to a message through the use of cryptographic techniques.” CAL. CODE REGS. tit. 2 § 22003(b)(1)(D) (1998).

[^41]: By including the term “process” as part of the definition of an electronic signature, both E-SIGN and UETA make clear that the “process” of clicking a mouse can qualify as a signature if the other applicable requirements are also present. As noted in the Reporter’s notes to UETA, “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 web site, 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 all the record of that process.” UETA Section 2, comment 7.

[^42]: For an overview of this technology and the process by which digital signatures are created, see Information Security Committee, Electronic Commerce Division, ABA Section of Science & Technology Law, Digital Signature Guidelines, August, 1996, available at www.abanet.org/scitech/ec/isc/dsgfree.html; Thomas J. Smedinghoff, Ed., Online Law, chs. 3, 4, 31 (Addison-Wesley, 1996); Warwick Ford and Michael Baum, Secure Electronic Commerce (Prentice Hall, 1997).

[^43]: Public key cryptography employs an algorithm using two different but mathematically related cryptographic keys. One key for creating a digital signature or transforming data into a seemingly unintelligible form, and the other key for verifying a digital signature or returning the message to its original form.

[^44]: In more technical terms, a digital signature is the sequence of bits that is created by running an electronic message through a one-way hash function to create a unique digest (or “fingerprint”) of the message and then using public key encryption to encrypt the resulting message digest with the sender’s private key.
This is, of course, not an exhaustive list of methods by which one can electronically sign a document. There are other ways of signing an electronic document, and presumably many more will be developed in the future. However, all forms of electronic signature must satisfy the three requirements outlined above. And each of these requirements raises some issues worthy of note for online transactions.

First, while the requirement that an electronic signature include any “sound, symbol or process” allows for the use of virtually any type of electronic signature, it is important to note that many forms of electronic signature can be inherently insecure. That is, for example, anyone can type someone else’s name, as long as they know how to spell it. Likewise, anyone can click on an “I accept” button. The key is in authenticating the person who applied the symbol or executed the process – i.e., in knowing (and being able to prove) who typed the name or who clicked on the “I accept” button. It’s like accepting an “x” as a signature on a paper contract. While a mark, such as an “x” may be a legally valid signature, it may not be very trustworthy. Trust is discussed in section 3 below.

Second, the requirement that the signature be “attached to or logically associated with” the record being signed requires that the parties to the electronic transaction implement an electronic recordkeeping process that, in the future, can provide evidence that a specific signature was applied to or used in connection with a specific document. The easiest way to do this is, of course, to have the signature incorporated as part of the electronic record that is stored. An alternative is to establish a demonstrably reliable and provable process whereby the signature (or evidence of the completion of a process) is stored separately from the electronic record being signed, but in a manner that will allow the two to be correlated in the event it is necessary for evidentiary purposes.

Third, the signature must be executed or adopted with the “intent to sign the record.” Thus, the signature needs to relate to a specific document, and evidence the signer’s intent with respect to that document. The signer’s intent, as with any transaction, is determined by the contents of the document and/or other surrounding facts and circumstances.

2.5 Ability to Retain Documents

Another key requirement for the enforceability of electronic transactions is that the documents be communicated in a form that can be retained and accurately reproduced by the receiving party. Specifically, the Federal E-SIGN legislation provides that the legal effect, validity, or enforceability of an electronic 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.”45 Likewise, UETA provides that “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.”46

This requirement does not, of course, limit electronic transactions to those parties that possess the technical capability for downloading or printing documents. Rather, the

45 E-SIGN Section 101(e).
46 UETA Section 8(c).
focus is on the form of the document as communicated by the sender, and essentially requires that the sender do nothing to inhibit the ability of the recipient to download, store, or print the applicable record. The fact that the recipient may choose to use a device without such capabilities (for example, a hand-held device without a print capability), should not affect the enforceability of the transaction. On the other hand, such provisions clearly call into question the form of click-wrap agreement typically used on many web sites in which the agreement is displayed in a separate window from which it cannot be downloaded or printed.

2.6 Record Retention Requirements

An essential element for the enforceability of all electronic transactions is recordkeeping. In the event of a dispute, it is necessary to produce reliable evidence documenting the terms of the transaction and the agreement to the parties. Similar requirements also exist, for example, to satisfy regulatory requirements (e.g., insurance regulations, securities regulations, banking regulations, etc.), as well as the requirements of government agencies, such as the IRS. For electronic transactions, the issue then becomes a question of whether keeping electronic records will satisfy applicable statutes, regulations, or evidentiary rules, and if so, what requirements must be met for acceptable electronic records.

Both E-SIGN and UETA address this issue directly, and impose similar requirements. Essentially, an electronic record will satisfy legal record retention requirements under UETA if the electronic record:

- 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
- remain accessible for later reference.\textsuperscript{47}

E-SIGN imposes a similar rule. That is, record retention requirements are met by retaining an electronic record of the information that:

- accurately reflects the information set forth in the contract or other record; and
- 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.\textsuperscript{48}

Both E-SIGN and UETA make clear that record retention requirements do not extend to information whose sole purpose is to enable the contract or other record to be sent, communicated, or received.\textsuperscript{49}

\textsuperscript{47} UETA Section 12(a).
\textsuperscript{48} E-SIGN Section 101(d).
\textsuperscript{49} E-SIGN Section 101(d)(2); UETA Section 12 (b).
3. Is the Transaction Trustworthy?\textsuperscript{50}

Beyond the threshold issue of legal enforceability, the second primary concern of parties to an electronic transaction is the pivotal question of trust. To say that an electronic transaction is enforceable (assuming it can be proven to the trier of fact) is one thing. To have a sufficient degree of trust in an electronic message such that one is willing to ship product, transfer funds, or enter into a binding contractual commitment in real time is something else. Trust is essential to electronic commerce, and it varies from transaction to transaction, largely depending on how high the stakes are. For example, the level of trust required for an online merchant to ship $200,000 worth of tires is much higher than what is required for an online bookstore to ship a $20 book. That’s because there’s a lot more riding on those tires. Likewise, a bank will require even greater assurances before it will make a multimillion-dollar funds transfer in real time in reliance on an electronic message.

The importance of trust for the success of e-commerce is widely recognized. For example, the Commission of the European Communities noted that:

The first objective is to build trust and confidence. For e-commerce to develop, both consumers and businesses must be confident that their transaction will not be intercepted or modified, that the seller and the buyer are who they say they are, and that transaction mechanisms are available, legal, and secure. Building such trust and confidence is the prerequisite to win over businesses and consumers to e-commerce.\textsuperscript{51}

Trust, of course, plays a role in virtually all commercial transactions. Regardless of whether the deal is struck in cyberspace or in the more traditional paper-based world, transacting parties must trust the messages that form the basis for the bargain. Trusting a message, from a legal perspective, requires consideration of the authenticity and integrity of the message, as well as an assessment of whether the message is nonrepudiable by the sender in the event of a dispute.

3.1 Authenticity — Who sent the message?

Authenticity is concerned with the source or origin of a communication.\textsuperscript{52} Who sent the message? Is it genuine or a forgery?

A party entering into an online transaction in reliance on an electronic message must be confident of the source of that message. For example, when a bank receives an electronic payment order from a customer directing that money be paid to a third party, the bank must be able to verify the source of the request and ensure that it is not dealing with an impostor.\textsuperscript{53}

\textsuperscript{50} Adapted from Thomas J. Smedinghoff, Ed., \textit{Online Law}, Chapter 3, by Lorijean G. Oei (1996).


\textsuperscript{52} See \textit{FED. R. EVID.} 901(a) (1995).

\textsuperscript{53} See \textit{U.C.C.} §§ 4A-202, 4A-203 & cmt. (1998).  Section 4A-202 solves this problem for a bank and its customer who has agreed to transact its banking electronically and to be subject to Article 4A.  \textit{Id.}  If the bank verifies the payment order by using a commercially reasonable security procedure, the customer will
Likewise, a party must also be able to establish the authenticity of its electronic transactions should a dispute arise. That party must retain records of all relevant communications pertaining to the transaction and keep those records in such a way that it can show that the records are authentic. For example, if one party to a contract later disputes the nature of its obligations, the other party may need to prove the terms of the contract to a court. A court, however, will first require that the party establish the authenticity of the record that the party retained of that communication before the court will consider it as evidence.\footnote{See, e.g., U.S. v. Eisenberg, 807 F.2d 1446 (8th Cir. 1986) (disputing the authenticity of letter); U.S. v. Grande, 620 F.2d 1026 (4th Cir. 1980) (disputing authenticity of invoice), cert. denied, 449 U.S. 830, 919 (1980).}

### 3.2 Integrity — Has the message been altered?

Integrity is concerned with the accuracy and completeness of the communication. Is the document the recipient received the same as the document that the sender sent? Is it complete? Has the document been altered either in transmission or storage?

The recipient of an electronic message must be confident of a communication’s integrity before the recipient relies and acts on the message. Integrity is critical to e-commerce when it comes to the negotiation and formation of contracts online, the licensing of digital content, and the making of electronic payments, as well as to proving up these transactions using electronic records at a later date. For example, consider the case of a building contractor who wants to solicit bids from subcontractors and submit its proposal to the government online. The building contractor must be able to verify that the messages containing the bids upon which it will rely in formulating its proposal have not been altered. Likewise, if the contractor ever needs to prove the amount of the subcontractor’s bid, a court will first require that the contractor establish the integrity of the record he retained of that communication before the court will consider it as evidence in the case.\footnote{See, e.g., Victory Med. Hosp. v. Rice, 493 N.E.2d 117 (Ill. App. Ct. 1986).}

### 3.3 Nonrepudiation — Can the message be Proved in Court?

Nonrepudiation is the ability to hold the sender to his communication in the event of a dispute.\footnote{See Information Security Committee, Electronic Commerce Division, ABA Section of Science & Technology Law, \textit{Digital Signature Guidelines}, August, 1996, available at www.abanet.org/scitech/ec/isc/dsgfree.html. One definition of nonrepudiation is “[s]trong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents.” \textit{Id.} at Section 1.20.} A party’s willingness to rely on a communication, contract, or funds transfer request is typically contingent upon having some level of comfort that the party can prevent the sender from denying that he sent the communication (if, in fact, he did send it), or from claiming that the contents of the communication as received are not be bound even if it did not in fact authorize the payment order. § 4A-202(b). If, however, the customer can prove that the person sending the fraudulent payment order did not obtain the information necessary to send such an order from an agent or a source controlled by the customer, the loss is shifted back to the bank. § 4A-203(a)(2). If the bank does not follow the security procedure and the order is fraudulent, the bank generally must cover the loss. § 4A-202(a).
the same as what the sender sent (if, in fact, they are what was sent). For example, a stockbroker who accepts buy/sell orders over the Internet would not want his client to be able to place an order for a volatile commodity, such as a pork bellies futures contract, and then be able to confirm the order if the market goes up and repudiate the order if the market goes south.\textsuperscript{57}

With paper-based transactions, a party can rely on numerous indicators of trust to determine whether the signature is authentic and the document has not been altered. These include using paper (sometimes with watermarks, colored backgrounds, or other indicia of reliability) to which the message is affixed and not easily altered, letterhead, handwritten ink signatures, sealed envelopes for delivery via a trusted third party (such as the U.S. Postal Service), personal contact between the parties, and the like. With electronic communications, however, none of these indicators of trust are present. All that can be communicated are bits (0s and 1s) that are in all respects identical and can be easily copied and modified.

This has two important consequences. First, in many cases it is difficult to know when one can rely on the integrity and authenticity of an electronic message. This, of course, makes difficult those decisions that involve entering into contracts, shipping products, making payments, or otherwise changing one’s position in reliance on an electronic message. Second, this lack of reliability can make proving up one’s case in court virtually impossible. For example, while a typewritten name appended at the end of an e-mail message may qualify as a signature under applicable law, that name could have been typed by anyone, and if the defendant denies the “signature” in a lawsuit, it may be virtually impossible for the plaintiff to prove the authenticity of that signature. As a result, nonrepudiation is by no means assured in such a case, and parties thus may choose to forego e-commerce in significant transactions where the risk of repudiation is too great.

In many respects, trust is a key element of the measurement of risk. And the need for trust can vary significantly, depending on the risk involved. Selling books on the Internet, for example, may not require a high level of trust in each transaction, especially where a credit card number is provided and the risk of loss from fraud is relatively low (e.g., a $20 book). On the other hand, entering into long-term, high-dollar value contracts electronically may require a much higher level of trust. At a minimum, the risk of a fraudulent message must be acceptable given the nature and size of the transaction.

Thus, where the amount at issue is relatively small or the risk is otherwise low, trust in an electronic message’s authenticity and integrity may not be a critical issue. If e-commerce is to reach its full potential, however, parties must be able to trust electronic communications for a wide range of transactions, particularly ones where the size of the transaction is substantial or the nature of the transaction is of higher risk. In such cases, a party relying on an electronic communication will need to know, at the time of reliance, whether the message is authentic, whether the integrity of its contents is intact, and, equally important, whether the relying party can establish both of those facts in court if a dispute arises (i.e., nonrepudiation).

\textsuperscript{57} See generally, John Browning, \textit{Follow the Money -- A New Stock Market Arises on the Internet}, SCI. AM. 31 (July 1995).
3.4 Establishing Trust Through Security Procedures

Establishing trust in an electronic transaction typically involves the use of a security procedure. A security procedure is "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 call-back or other acknowledgement procedures."\(^{58}\) Because they are designed to either verify the identity of the sender of an electronic record, or to detect error in or alteration of an electronic record, security procedures can also have a legal effect.

There are a number of security procedures that can be used to assist in establishing trust for electronic communications. These include:

- a digital signature;
- replies and acknowledgments;
- repeat-back acknowledgments;
- the use of a process or system that produces a demonstrably trustworthy document;\(^{59}\)
- date/time stamping;
- the use of trusted third parties; and
- encryption.

**A Digital Signature.** A handwritten signature on a paper document purporting to originate from an identified source can authenticate a communication if that signature is shown to be genuine. Of course, an electronic communication cannot bear a traditional handwritten signature, but it may bear a digital signature or other digital equivalent. If a digital signature can be verified using a public key that is reliably associated with the sender, the recipient can obtain a high degree of assurance that the communication must have come from the sender.\(^{60}\) Only the sender’s public key can decrypt a digital signature encrypted using the sender’s private key. Furthermore, assuming the sender’s key has not been lost or compromised, the sender cannot deny having sent it. Thus a digital signature can provide a means of identifying the source of a communication and preventing a sender from repudiating that communication. A digital signature can also be used to verify the integrity of an electronic communication. If the recipient can verify the sender’s digital signature, the integrity of the communication has been shown.

**Replies and Acknowledgments.** Computer systems are particularly well suited to screening incoming communications and sending a return acknowledgment to the

\(^{58}\) UETA Section 2(14).


purported sender. A log showing what was received, the identified sender, the fact that an acknowledgment was sent to the sender, and that the acknowledgment was not rebuked will help authenticate the source of a communication. Sending and retaining records of acknowledgments as well as of any responses repudiating those acknowledgments can also enhance the authenticity of communications.

A reply to an earlier communication tends to authenticate that reply. For example, if a buyer offers in a letter to purchase 500 gross of #3 widgets from the seller for $1500, and the seller counteroffers in a letter saying, “I will sell the #3 widgets for $1775”, the authenticity of the seller’s letter is supported. By preserving a record of the course of the correspondence, each of the documents can be authenticated. This technique works equally well for paper-based and electronic communications.

**Repeat-Back Acknowledgments.** The technique of sending an acknowledgment to establish an electronic communication’s authenticity can be taken one step further to establish the integrity of a communication. With electronic communications, it is a simple matter not only to send an acknowledgment, but to repeat the entire contents of the communication back to the purported sender. If the repeat-back acknowledgment is different than the original communication, the sender can alert the recipient. The sender will want to be sure to create and retain a record of the communication as received, the repeat-back acknowledgment, and any repudiation of the repeat-back acknowledgment it received or a notation that none was received.

**Process or System.** Because electronic communications do not always have the same identifying characteristics as paper communications do, it is helpful to resort to other techniques for establishing authenticity that are specially suited to electronic communications. These techniques all involve the use of a computer system to perform automated recordkeeping functions. For example, if a company has configured its computers to automatically archive an electronic record copy of the communications it creates and receives, this may help establish that the records of those communications are genuine. Adopting system security controls that limit access to archival copies can further ensure the authenticity of such archival record copies. The use of such system security measures can help a company to demonstrate the integrity of its records.

Another technique is to configure the user’s computers to create a log of all incoming and outgoing communications and to cross-reference this log information to archived records. Log information showing the source of the record and the time of its creation or receipt provides further proof of its authenticity.

**Date/Time Stamping.** A digital date/time-stamp provides another way to verify that a communication has not been changed. A date/time-stamp is issued for a message digest of the communication. This fixes the content of the message digest as of a certain date. To later verify the integrity of the communication another message digest is created for the communication. If it matches the date/time-stamped message digest, the communication has not been changed.

**Trusted Third Parties.** A party can establish the integrity of a communication by sending and receiving all of its electronic communications through a neutral third party that can retain a copy of each communication. Assuming that this third party is

---

trustworthy, each party can then rely on the third party in the event that the integrity of a record of a communication is questioned.

Encryption. If a sender wants to send an electronic communication to a recipient and keep it confidential, the sender can encrypt the communication.

The security measures that can be taken to help ensure that electronic communications and records are trustworthy may not yet be readily accepted, but their legal effectiveness is already being recognized. The first formal recognition of the legal effect of security procedures occurred in 1989 with the approval of Article 4A of the UCC. 62

Article 4A addresses the electronic transfer of funds by wire 63. A person who wishes to transfer funds electronically does so by transmitting an electronic message, called a payment order, to his bank. Because that message cannot bear a traditional ink signature or other paper-based security measure, security procedures must be used instead. The UCC recognized this and the reality that a bank receiving a payment order needs something objective on which it can rely in determining whether it may safely act on that order. 64 Article 4A modernized the law by providing that a bank could rely on security procedures as a substitute for the traditional time-tested requirement of a signature. Under Article 4A, an electronic message instructing a bank to transfer funds to a payee is considered valid, and the bank is authorized to transfer the funds in accordance with the order if (1) the bank’s customer actually authorized the order or (2) if the authenticity and integrity of the order is “verified” pursuant to a “commercially reasonable” security procedure regardless whether the order was actually authorized by that person. The bottom line is that Article 4A adopts “security procedures” rather than “signatures” as the basis for verifying transactions and apportioning liability.

3.5 The Law and Trust in E-Commerce

Most electronic signature statutes simply do not address the issue of trust at all. This includes both E-SIGN and UETA. Those statutes that do focus on the issue take two different approaches.

Under the first approach, a trustworthy electronic signature is a precondition to enforceability as a signature. Statutes adopting this approach typically require that electronic signatures possess four attributes – i.e., the electronic signature must be: (1) unique to the person using it; (2) capable of verification; (3) under the sole control of the person using it; and (4) linked to the data in such a manner that if the data is changed, the signature is invalidated. 65 If all of these requirements are met, the electronic

62 See U.C.C. Art. 4A, Funds Transfers (1989). Article 4A has been adopted in forty-seven states.
64 U.C.C. § 4A-203 Official Comment.
65 See ALASKA STAT. § 09.25.510 (Michie 1999) (applying generally to all communications); CAL. GOVT CODE § 16.5 (West, 1999) (limiting application to communications with public entities); GA. CODE ANN. § 10-12-4 (Michie 1998) (applying generally to all communications); IDAHO CODE § 67-2357 (1998) (limiting application to the filing and issuing of documents by and with state and local agencies); 15 ILL. COMP. STAT. 405/14.01 (1997) (limiting application to communications between a state agency and the comptroller); 205 ILL. COMP. STAT. 705/5 (West 1998) (limiting application to communications between financial institutions and their customers); IOWA CODE ANN. § 1555A.27 (West 1999) (limiting application to prescriptions); KAN. STAT. ANN. § 60-2616 (1997) (applying generally to all communications); KY. REV.
signature will be deemed to be a signature for purposes of that state’s various statutory and regulatory signature requirements within the scope of the statute – i.e., the electronic signature will be enforceable. In the U.S., statutes adopting this approach are preempted by E-SIGN.\(^66\)

A number of other statutes have adopted a second approach. These statutes provide that almost any form of electronic signature can be enforceable and meet legal signature requirements, while recognizing that some electronic signatures are more trustworthy than others.\(^67\) To encourage the use of those electronic signatures deemed to be more trustworthy, and to provide message recipients with an enhanced level of assurance at the time of reliance regarding the authenticity and integrity of messages using such signatures, these statutes typically provide a legal benefit in the form of an evidentiary presumption regarding the sender’s identity and/or the integrity of the document. Yet there is an argument that these statutes too are preempted by E-SIGN.

Some of these statutes take a technology-neutral approach to identifying the class of trustworthy electronic signatures that qualify for such a legal benefit. For example, the Illinois Electronic Commerce Security Act creates a class of trustworthy signatures called “secure electronic signatures.”\(^68\) An electronic signature that qualifies as a secure electronic signature enjoys a rebuttable presumption that the signature is that of the person to whom it correlates.\(^69\) Similar types of presumptions for a technology-neutral class of secure records and secure signatures appear in legislation that has been enacted in Iowa.\(^70\) Other technology-neutral electronic signature legislation incorporating rebuttable presumptions (although limited to certain types of transactions) has been enacted in Alabama (limited to certain tax-related usage)\(^71\) and in Ohio (limited to certain health care usage).\(^72\)

---

\(^66\) E-SIGN Section 101(a).

\(^67\) Electronic signatures, like traditional signatures of ink on paper, come in varying degrees of security. A handwritten signature, for example, is more trustworthy than an “X,” and a notarized signature is more trustworthy than both. Just as the law provides certain benefits to the more trustworthy forms (see e.g., FED. R. EVID. 901(a) (1995), (confirming that notarized signatures are considered self-authenticating), these electronic signature statutes seek to define the characteristics required for a trustworthy (or secure) signature.


\(^69\) 5 ILL. COMP. STAT. 175/10-120.


\(^71\) ALA. CODE § 40-30-5 et seq. (1999).

\(^72\) OHIO REV. CODE ANN. § 3701.75 (West 1999).
Technology-specific statutes that confer similar legal presumptions have been enacted in Minnesota, Missouri, Utah, and Washington, and all such statutes focus solely on digital signature technology. To ensure that the digital signature possesses a level of trust sufficient to warrant enhanced legal recognition, these statutes impose a regulatory structure on certification authorities who voluntarily elect to be licensed by the State. Based on the apparent assumption that all certificates issued by licensed certification authorities are trustworthy, and that a digital signature that is created using the private key corresponding to the public key listed in such a certificate is a trustworthy signature, the legislation has bestowed attributes of trust to messages verifiable by such certificates.

For electronic transactions, presumptions of the signer’s identity and of message integrity can help to provide necessary assurances to relying parties, thereby enabling them to engage in online commercial activities with confidence that their transactions will be easier to enforce in court if that should be necessary. Such presumptions can provide the predictability and trust necessary to rely on a message, and act accordingly, in real time. Such presumptions are based on the trustworthiness of the security procedure used to create the electronic signature, and the fact that the purported sender is more likely than the recipient to possess the information necessary to prove or disprove the validity of the signature.

Yet the use of presumptions in electronic signature legislation is an issue that has generated rather extensive controversy. Criticism has centered on concerns that consumers and small businesses that lack an understanding of the sophisticated technologies used to create the secure electronic signature may unwittingly find themselves in a situation where their failure to protect the security of their signature device (e.g., their private key) will expose them to substantial liability for unauthorized transactions made by persons who unlawfully obtained access to their signature device.

Moreover, there is an argument that such presumptions are preempted by E-SIGN on the ground that they “accord greater legal status or effect to the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures.”

---


24 See, e.g., MINN. STAT. ANN. § 325K.20; MO ANN. STAT. § 28.677; UTAH CODE ANN. § 46-3-101; WASH. REV. CODE § 19/34/100. The digital signature legislation enacted in Germany, Italy, and Malaysia contains a similar approach.

25 See, e.g., UTAH CODE ANN. § 406(3). The Utah Digital Signature Act provides that if a digital signature is verified by the public key listed in a valid certificate issued by a licensed certification authority, then a court of the State of Utah “shall presume that”: (a) the digital signature is the digital signature of the subscriber listed in that certificate, and (b) the digital signature was affixed by that subscriber with the intention of signing the message. Id.

26 See also Reporter to the Uniform Electronic Transactions Act Drafting Committee, Memorandum (Sept. 18, 1998) <http://www.law.upenn.edu/library/ulc/uecicta/eta1098m.html> (discussing some of the reasons favoring and disfavoring the use of presumptions in electronic signature legislation).

27 E-SIGN Section 102(a)(2)(A)(ii).
4. What Rules Govern the Transaction?

For any electronic transaction, we need to know the rules that govern the use of the electronic medium of communication and storage. And these rules can differ significantly from those that govern transactions documented on paper. For example, when laws or regulations require the delivery of “written” documents, require that such documents be delivered by “first-class mail,” or require that documents be in a certain form (such as on 8-1/2” x 11” paper), how do those requirements translate to the e-commerce world? Likewise, what are the rules regarding the time and place of sending and receipt of electronic documents? How can we notarize or acknowledge an electronic document? What is the effect of errors introduced into the communication process? What new provisions are required to protect consumers in an electronic environment? Are clickwrap agreements enforceable? Can they incorporate by reference lengthy documents accessible by a hyperlink? To engage in electronic transactions, requires an understanding of these rules.

Unfortunately, most electronic transaction statutes enacted to date say nothing about the rules governing the conduct of parties using electronic records and signatures. However, UETA, and to a lesser extent E-SIGN, do provide guidance with respect to some of the rules that will govern electronic transactions.

4.1 Timing Rules

When is an electronic record considered sent? When is it considered to have been received? These issues of timing can be important for resolving a variety of issues, such as whether a binding contract has been created (particularly in the case where a contract offer sets a deadline for acceptance), whether a document has been filed with the applicable government agency on time, when a trade was consummated, and so forth. For example, in one case, a fax transmission was not effective notice, because while it was started before the deadline passed, it was not completed until afterwards.\(^78\) Electronic transmissions may pose similar problems, especially since there can be a delay between sending and receipt.

UETA provides that the time at which an electronic record is considered to have been sent is the time that the record “enters an information processing system outside the control of the sender” (in the case where a message is sent from one computer system to another), or “enters a region of the information processing system designated or used by the recipient which is under the control of the recipient” (in the case where a message is sent from one person to another on the same system, such as AOL).\(^79\) An electronic record will be considered to have been sent as of that time, provided that it is addressed properly to an information processing system that the recipient has designated or uses for the purpose of receiving electronic records and from which the recipient is able to retrieve the electronic record, and provide further that it is in a form capable of being processed by that system.\(^80\)

---

78 Bomen Inc., Comp Gen B-234652, May 17, 1989, 3 CGEN (CCH) ¶ 103, 198 (1989) (23 page fax started, but not completed, before the deadline).

79 UETA Section 15(3).

80 UETA Section 15(a)(1) and 15(a)(2).
Conversely, UETA provides that an electronic record is considered *received* by the intended recipient when it enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic records of the type sent and from which the recipient is able to retrieve the electronic record, and is in a form capable of being processed by that system.\(^{81}\) It is also important to note that an electronic record is considered received even if no individual is aware of its receipt. That is, as with first class mail, once the message is delivered it makes no difference whether or not the addressee actually opens it.

### 4.2 Venue Rules

Another important question, and one that may have a bearing on determining which law applies to a transaction, is the question of “where” a message is considered sent from or received at. E-SIGN does not address this issue.

UETA provides, as a default rule, that 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.\(^{82}\) If the sender or recipient has more than one place of business, the relevant place of business is considered to be the one that has the closest relationship to the underlying transaction. If the sender or the recipient does not have a place of business, then the place of business is considered to be the sender’s or recipient’s residence, as the case may be.\(^{83}\)

### 4.3 Requirements for Creation of Electronic Contracts

A contract may be made in any manner sufficient to show agreement, including offer and acceptance, or conduct that recognizes the existence of a contract.\(^{84}\) In theory, the same rule should apply to electronic contracts.

A variety of procedures are available for forming electronic contracts. They include:

- **E-mail:** Offers and acceptances may be exchanged entirely by e-mail, or can be combined with paper documents, faxes, and oral discussions.

- **Web Site Forms:** In many cases a Web site operator will offer goods or services for sale, which the customer orders by completing and transmitting an order form displayed on screen.

- **Click Through Agreements:** A merchant may offer products, data, software or digital content online, subject to a form agreement accepted by clicking on an “I Accept” button. The user’s conduct of downloading the content may constitute acceptance of the form agreement.

---

81 UETA Section 15(b).
82 UETA Section 15(d).
83 UETA Section 15(d).
84 UCC 2-204.
• Electronic Data Interchange ("EDI"): EDI involves the direct electronic exchange of information between computers; the data is formatted using standard protocols so that it can be interpreted and implemented directly by the receiving computer. EDI is often used to transmit standard purchase orders, acceptances, invoices, and other records, thus reducing paperwork and the potential for human error.

• Electronic Agents: An electronic agent is software that is used independently to initiate an action or respond to electronic messages or performances without intervention by an individual at the time of the action, response or performance.85

Contract offers may be made orally, in writing, or by conduct. There is no reason why an electronically transmitted offer should be any less effective than an oral or written one.86 To be valid, an offer must communicate to the person receiving it that, once the offer is accepted, a contract is created.

An offer may be accepted "in any manner and by any medium reasonable in the circumstances."87 Typical offline acceptances include written and oral communications, as well as acceptance by conduct. Their online counterparts include acceptance by e-mail or other form of electronic message, by electronic agent, and by conduct such as clicking on a button or downloading content.

Thus, if an offer is made by e-mail, one should be able to accept it by the same means.88 But what if the offer was made by some other method, such as letter or fax? An acceptance does not necessarily have to be sent the same way as the offer.89 However, UETA provides that an electronic record is considered received only when it enters a computer system "that the recipient has designated or uses for the purpose of receiving electronic records of the type sent."90 Thus, if the parties have regularly corresponded in the past by e-mail, an e-mail acceptance sent to the offerors e-mail address will presumably be effective. However, in some cases many people have multiple e-mail addresses that are used for different purposes, and some of these e-mail addresses may be rarely used or monitored. Thus, the purpose of the foregoing requirement is to assure that recipients can designate the e-mail address or system to be used in a particular transaction.

85 See UETA Section 14.
86 Of course, there can be questions about the reliability of electronic communications, which may make it more difficult to introduce evidence in court. Information security matters are discussed below.
87 UCC 2-206(1)(a). See also Uniform Computer Information Transactions Act, Section 203(1) (approved for enactment, July 29, 1999), available at www.law.upenn.edu/library/ulc/ulc.htm, which restates the general rule that an offer to make a contract invites acceptance in any manner and by any medium reasonable under the circumstances.
88 It is well established that an acceptance may properly be sent by the same means as the offer, unless the offer says otherwise. See Restatement (Second) of Contracts § 65.
89 See e.g. Market Development Corp. v. Flame-Glo Ltd., 1990 WL 116319 (E.D. Pa. August 8, 1990) (a mailed offer may be accepted by fax).
90 UETA Section 15(b)(1).
4.4 Automated transactions — Rules for Electronic Agents

Can the act of a computer (without human involvement) create a contract? The answer should be yes, depending on the circumstances.

A computer can generate an offer. For example, an inventory system can calculate when supplies are low, and automatically generate an electronic purchase order to the vendor. Would such an order be a binding offer? While there are not yet any cases directly on point, one analogous case has upheld the validity of a computer generated insurance renewal. The court, reasoning that the computer operates only in accordance with the information and directions supplied by its programmers, held the insurance company was bound by the computer-generated renewal notice.

Acceptances can also be generated by computer. The issue, however, is likely to be whether a responsive message is an acceptance or merely an acknowledgment of receipt. In most cases it will depend on the nature of response. For example, in one case involving a computer order entry system, orders were placed by touch-tone phone, and the system automatically generated a tracking number for each order. When the seller refused to fill the buyer's order, the buyer sued. The court held that no contract had been created, since the tracking number was merely for administrative convenience, and not a clear acceptance.

This issue will certainly arise in EDI transactions, where a computer can automatically acknowledge receipt of an electronic purchase order. However, this type of acknowledgment usually only means the computer received the message in a form it could read. It does not necessarily mean the order was accepted. Other types of EDI messages, such as purchase order acknowledgments, would be proper acceptances. UETA also provides that receipt of an electronic acknowledgement from a computer establishes that a record was received by the computer, but does not, by itself, establish that the content sent corresponds to the consent received.

Relatedly is the question of the enforceability of contracts formed via electronic agents. An electronic agent is a computer program or other automated means used to initiate an action or respond to electronic records or performances in whole or in part without review or action by an individual at the time of the action or response.

Both E-SIGN and UETA also specifically recognize the validity of contracts formed by electronic agents. E-SIGN provides that a contract or other record relating to a transaction 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

---

91 State Farm Mutual Auto. Ins. Co v. Brockhurst, 453 F.2d 533 (10th Cir. 1972)
92 Corinthian Pharmaceutical Systems v. Lederle Labs, 724 F. Supp. 605 (S.D. Ind. 1989). The seller's other correspondence stated that orders were not effective under accepted by the seller.
93 An EDI “functional acknowledgment” confirms that the message was functionally complete - that is, all fields in the form were completed with recognizable codes. It does not reflect acceptance of the substantive terms.
94 UETA Section 15(f).
95 See E-SIGN Section 106(3); UETA Section (2)(6).
bound. Likewise, UETA recognizes the enforceability of contracts formed through the interaction of electronic agents. First, UETA recognizes that 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 agent's actions or the resulting terms and agreements. In addition, however, UETA also recognizes that a contract may be formed by the interaction of an electronic agent and an individual.

4.5 Errors in transmission

Another key concern for electronic transactions is the problem of changes or errors that may be introduced into an electronic record, either because of system or transmission problems, or intentional alteration.

E-SIGN does not address this issue. However, UETA does contain a limited provision. As a general rule, UETA provides that if the parties have agreed to use a security procedure to detect changes or errors in electronic records, and one party conforms to the procedure but the other does not, if an error or change occurs that could have been detected by the non-conforming party had that party conformed to the procedure, the conforming party may avoid the effect of the changed or erroneous record. Also, in the case of an automated transaction involving an individual, the individual may avoid the effect of a record that resulted from an error made by the individual if the electronic agent of the other party did not provide an opportunity for the prevention or correction of the error, and the individual promptly notifies the other person of the error, takes reasonable steps to return or destroy the consideration received as a result of the erroneous record, and has not used or received any benefit or value from the consideration received, if any.

4.6 Notarization or witness requirements

In many cases, a law requires that a signature or a document be notarized, acknowledged, verified, or made under oath. Both UETA and E-SIGN recognize that this requirement can also be satisfied for electronic transactions, so long as the electronic signature of the person authorized to perform these 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. However, it is important to note that this provision does not eliminate any of the other requirements of notarial laws (such as the use of a stamp or seal). It simply allows the signing of the document to be accomplished in an electronic medium. Some states, such as Florida, have already passed electronic notary statutes designed to address how the other requirements of a notary can be accomplished in an electronic medium. However, for states that have not, the value of this provision may be limited.

---

96 E-SIGN Section 101(h).
97 UETA Section 14(1).
98 UETA Section 14(2).
99 UETA Section 10(1).
100 UETA Section 10(2).
101 E-SIGN Section 101(g); UETA Section 11.
4.7 Party Autonomy

With the law in a state of flux, one common approach for parties engaged in e-commerce is to simply enter into their own contract to decide the rules that will govern the conduct of their e-commerce transactions. This concept of party autonomy – i.e., the right of the parties to agree between themselves as to the rules that govern their transactions – is a core premise of the U.S. international position regarding electronic commerce. In the Framework for Electronic Commerce (released by the Clinton administration on July 1, 1997), the U.S. position is stated as “parties should be free to order the contractual relationship between themselves as they see fit.”

Consistent with this view, UETA expressly provides that, subject to certain exceptions, the effect of any of the provisions in UETA may be varied by agreement. E-SIGN, however, like most other legislation, however, is simply silent on the subject of party autonomy. And some legislation, like consumer protection legislation, actually prohibits variation by agreement. Moreover, the common law is not always clear on this point.

Generally, under the common law, the courts look more favorably on agreements between parties regarding evidentiary matters that are entered after litigation has commenced than on pre-litigation contracts. However, courts do uphold many pre-litigation contract provisions that affect later litigation matters. Thus, for example, courts today uniformly enforce arbitration clauses in contracts, even though such provisions withdraw a court’s power to decide the parties’ dispute. Likewise, forum selection clauses are enforceable if reasonable (although they cannot override exclusive federal court jurisdiction pursuant to federal statutory law). Courts also enforce integration and merger clauses in contracts, which prohibit the court from considering oral evidence to alter the terms of a written contract.

---

102 See www.ecommerce.gov/framewrk.htm.
103 UETA Section 5(d).
104 See United States v. Mezzanatto, 513 U.S. 196, 115 S. Ct. 797, 802, fn. 3 (1995) (“...it is true that extrajudicial contracts made prior to litigation trigger closer judicial scrutiny than stipulations made within the context of litigation.”). Thus, the courts have approved stipulations that have waived hearsay objections, (Sac And Fox Indians of Mississippi in Oklahoma, 220 U.S. 481, 488-489 (1911)) have held that stipulations as to the admissibility of documents precludes subsequent objections as to authenticity (Tupman Thurlow Co. v. S.S. Cap Castillo, 490 F.2d 302, 309 (2nd Cir. 1974); United States v. Wing, 450 F.2d 806, 911 (9th Cir. 1971)), and have held that a stipulation to admissibility precludes a hearsay objection at trial (United States v. Bonnet, 877 F.2d 1450, 1458-1459 (10th Cir. 1989). Courts also have approved stipulations to waive the best evidence rule (Finch, Van Slyk & McConville v. Le Sueur County Co-op Co., 128 Minn. 73, 150 N.W. 226 (1914); Skibsaktieselskapet Bestum III v. Duke, 131 Wash. 467, 230 P. 650 (1924)), or to waive the qualifications of an expert witness (Brinck v. Bradbury, 179 Cal. 376, 176 P. 690 (1919)).
105 See Note, Contracts to Alter the Rules of Evidence, 46 Harv. L. Rev. 138, 139 (1933).
Thus, it appears that parties may contract regarding evidentiary matters prior to litigation as long as those matters do not infringe on the fact-finding and discretionary powers of the trial court. The Supreme Court stated that “[a]bsent some ‘overriding procedural consideration that prevents enforcement of the contract,’ courts have held that agreements to waive evidentiary rules are generally enforceable even over a party’s subsequent objections.”

The Court stated, however, that “there may be some evidentiary provisions that are so fundamental to the reliability of the fact-finding process that they may never be waived without irreparably discrediting the … courts.”

Cases have upheld the waiver of the physician-patient privilege in an application for insurance. Courts have upheld provisions in insurance policies that preclude liability for death or injury caused by a firearm unless the accidental cause is first established by the testimony of an eyewitness other than the insured or claimant. And, some courts have upheld provisions in insurance policies that alter the presumption of death after absence for seven years, although many other courts refuse to enforce such agreements. Finally, in one case, the parties agreed, in settlement of litigation that they would abide by the results of a polygraph test and that if the witness was not truthful, there would be no claim to the monies allegedly owed. When a claim was filed but the witness refused to take a polygraph test, the court enforced the parties’ agreement and dismissed the action.

On the other hand, other provisions in pre-litigation contracts have been held unenforceable. For example, in one case, the court refused to enforce an agreement that only certain types of appraisals were admissible, on the ground that such a provision “purported to totally preempt the court from its consideration of legally competent evidence.” In another case, the court held that a licensee could dispute a contractual recital that trademark infringement was conclusive evidence of irreparable injury. And in another case, the court stated that “It is at best highly doubtful that parties may, by contract, allocate burdens of proof, establish standards of proof, or, in other respects, control judicial fact-finding procedures in actions arising out of their contracts.” Finally, the Michigan Supreme Court has held that the parties could not by contract change the required procedures for arbitration under Michigan law.

---


110 Mezzanatto, 513 U.S. 196, 115 S. Ct. at 803.

111 See Adreveno v. Mutual Reserve Fund Life Association, 34 F. 870 (E.D. Mo. 1888); Lincoln National Life Insurance Co. of Fort Wayne v. Hammer, 41 F.2d 12 (8th Cir. 1930); Wirthlin v. Mutual Life Insurance Co., 56 F.2d 137 (10th Cir. 1932).


114 Omni Investment Corp. v. Cordon International Corp., 603 F.2d 81 (9th Cir. 1979).


Unfortunately, the case law regarding pre-litigation contracts provides little guidance in deciding whether the agreements regarding electronic signatures or attribution procedures are enforceable. To the extent that those cases establish any general principal at all, it appears to be that courts are fairly amenable to enforcing agreements that affect matters of procedure or evidence but will not enforce agreements that ignore or change substantive law or restrict the court’s authority to apply the substantive law of contracts.