The Legal Requirements for
CREATING SECURE AND ENFORCEABLE ELECTRONIC TRANSACTIONS

August 30, 2002

Thomas J. Smedinghoff
Baker & McKenzie
130 East Randolph Drive
Chicago, Illinois 60601
312-861-8670
312-961-2899 (fax)
smedinghoff@bakernet.com

TABLE OF CONTENTS

Page

The Legal Requirements for
Creating Secure and Enforceable
Electronic Transactions

Thomas J. Smedinghoff [1]
Baker & McKenzie

What are the rules and requirements for conducting business transactions in electronic form? 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 the Internet becomes an integral part of business, there is an ever-increasing desire to conduct these transactions in that electronic medium. This article 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 largely the same worldwide.

Like all transactions, electronic transactions involve documents (usually referred to as "records,"[2] "electronic records"[3] or "data messages"[4]), and signatures (usually referred to as "electronic signatures"[5]), that are created, communicated, and stored in electronic form.[6] They

---

[1] Thomas J. Smedinghoff is a partner with the law firm of Baker & McKenzie and North American Coordinator of the Firm's Electronic Commerce Law Practice. He was chair of the Illinois Commission on Electronic Commerce and Crime and author of the Illinois Electronic Commerce Security Act, 5 Ill. Comp. Stat. 175. He was the 1999-2000 chair of the American Bar Association ("ABA") Section of Science & Technology Law, and is the current chair of the ABA Electronic Commerce Division. He is a member of the U.S. Delegation to the United Nations Commission on International Trade Law ("UNCITRAL"), through which he participates in its Working Group on Electronic Commerce that is drafting international electronic commerce legislation, and is the editor and primary author of the book on electronic commerce titled: ONLINE LAW (1996).

[2] The term "record" is typically defined as "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form." *See* Electronic Signatures in Global and National Commerce Act ("E-SIGN"), at 15 U.S.C. § 7006; Uniform Electronic Transaction Act ("UETA"), at § 2(13).

[3] The term "electronic record" means a "record created, generated, sent, communicated, received, or stored by electronic means." E-SIGN, 15 U.S.C. § 7006 (4); UETA § 2(7).

[4] The term "data message" means "information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, Electronic Data Interchange (EDI), electronic mail, telegram, telex, or telecopy." UNCITRAL Model Law on Electronic Signatures, Article 2(c).

[5] The term "electronic signature" means "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. E-SIGN, 15 U.S.C. § 7006 (5); UETA § 2(8). Under the European Union Electronic Signature Directive, "electronic signature" means "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication." Electronic Signatures Directive, 1999/93/EC (13 December 1999), Article 2(1).

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., by using software or a so-called "electronic agent"), or through human interaction with a computer (e.g., when an individual accesses a web site and enters into a purchase agreement). Electronic transactions 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. Frequently, 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. Legal Recognition of Electronic Transactions

The threshold question for any type of transaction is whether it will be legally valid and enforceable if done in electronic form. Answering this question requires consideration of the legal barriers that might exist with respect to that type of transaction, and any additional requirements for enforceability that might be imposed by law solely because of the electronic nature of the transaction. For purposes of discussion, we will assume that the fundamental legal elements required for that type of transaction are otherwise present and satisfied. For example, if the electronic transaction involves entering into a contract, this article assumes that the basic requirements of a contract – e.g., offer, acceptance, consideration, etc. – are present, and focuses only on the additional requirements for enforceability that arise because of the electronic nature of the transaction.

1.1 Legal Barriers to E-Commerce

When the enforceability of electronic transactions was first considered, a variety of concerns were raised. There were, for example, many questions regarding whether electronic records and electronic signatures satisfy writing and signature requirements imposed by a variety of statutes and regulations; whether records maintained solely in an electronic form will satisfy legal record keeping requirements; whether the record keeper can establish the authenticity and integrity of such records; whether an electronic record constitutes an "original" for evidentiary purposes;[7] and whether electronic records and electronic signatures would be denied admissibility in court because of their electronic form.

---

[6] "Electronic" form means "relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities." E-SIGN, 15 U.S.C. § 7006 (2); UETA § 2(5). See, also, 5 Ill. Comp. Stat. 175/5-105 (1998).

[7] The requirement that a document be "an original" occurs in a variety of contexts for a variety of reasons. In many situations, documents must be transmitted unchanged (i.e., in their "original" form), so that other parties may have confidence in their contents. Examples of documents where an "original" is often required include trade documents (e.g., weight certificates, agricultural certificates, quality/quantity certificates, inspection reports, insurance certificates) and non-business related documents (e.g., birth certificates and death certificates). When these documents exist on paper, they are usually only accepted if they are "original," because alterations may be difficult to detect in copies.

The requirement that a document be "an original" is also important from an evidentiary perspective. In particular, the "best evidence rule" (sometimes referred to as the "original document rule") requires that:

The biggest issue, by far, has focused on the writing and signature requirements imposed by various laws. Specifically, in many cases, the law requires that a transaction be both documented in "writing,"[8] and "signed" by the person who is sought to be held bound, in order for that transaction to be enforceable. The Statute of Frauds is, of course, the best example of such a law.[9] In addition, in the U.S. 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. For example, Georgia has over 5,500, and Ohio has over 8,000, of such statutory sections.[10]

Statutes and regulations that require transactions to be "in writing" and "signed" have generally been perceived to constitute legal barriers to electronic transactions. The concern is that an electronic record might not qualify as a "writing," and an electronic signature might not qualify as a "signature." In other words, many felt that such writing and signature requirements are satisfied only by ink on paper. This general concern about the "legality" of electronic records and electronic signatures has persisted, not only because of a few contrary court decisions,[11] but also because of a lack of specific statutory authorization.

> In proving the terms of a writing, where the terms are material, the original writing must be produced unless it is shown to be unavailable for some reasons and other than the serious fault of the proponent.

1 McCormick on Evidence §230 at 704 (Cleary Ed., 3d ed. 1984). See also Federal Rule of Evidence 1002 "Requirement of Original" which states that "to prove the content of a writing, recording or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by act of Congress."

[8] 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, UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, at par. 48, available at www.un.or.at/uncitral/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.bmck.com/cecc-fin.doc.

[9] 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.

[10] See Report of the National Conference of Commissioners on Uniform State Laws (NCCUSL), Uniform Electronic Transactions Act, Task Force on State Law Exclusions, (Sept. 21, 1998), www.webcom.com/legaled/ETAForum/docs/report4.html.

[11] See, e.g., Department of Transportation v. Norris, 474 S.E.2d 216 (Ga. Ct. App. 1996), rev'd sub nom., Norris v. Georgia Dept of Transportation, 486 S.E.2d 826 (1997) (holding that a fax transmission was not a writing).

1.2 The Legislative Response

As a consequence, the enforceability of electronic transactions has been the subject of extensive legislative efforts. The U.S. Federal Government, all 50 U.S. states, 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.[12]

- In the U.S., the enforceability of electronic transactions is primarily governed by the Electronic Signatures in Global and National Commerce Act ("E-SIGN"),[13] a federal law enacted in 2000 that largely preempts inconsistent state law, and the Uniform Electronic Transactions Act ("UETA"),[14] a uniform state law that was finalized by the National Conference of Commissioners on Uniform State Laws ("NCCUSL") in 1999 and has now been adopted by 40 states.[15]
- In the European Union, the enforceability of electronic transactions is governed by the Electronic Signatures Directive adopted in 1999,[16] and the Electronic Commerce Directive adopted in 2000.[17]
- Internationally, model laws governing the enforceability of electronic transactions have also been developed by the United Nations Commission on International Trade Law ("UNCITRAL") Working Group on Electronic Commerce,[18] which completed

---

[12] See Baker & McKenzie, Global E-Commerce Law Web site www.bakernet.com/ecommerce (providing a regularly updated summary of e-commerce legislation).

[13] Electronic Signatures in Global and National Commerce Act (hereinafter "E-SIGN"), S. 761, P.L. 106-229, 15 U.S.C. 7001 *et. seq*., effective October 1, 2000. E-SIGN is available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_bills&docid=f:s761enr.txt.pdf. E-SIGN preempts all inconsistent state legislation, other than state enactments of UETA in the form promulgated by NCCUSL.

[14] Uniform Electronic Transactions Act (hereinafter "UETA"), approved by the National Conference of Commissioners on Uniform State Laws (NCCUSL) on July 23, 1999. A copy of UETA is available at www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm.

[15] As of September 1, 2002, 40 states and the District of Columbia had enacted UETA. For an updated list of those states that have enacted UETA, see http://www.bakernet.com/ecommerce/uetacomp.htmwww.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-ueta.asp.

[16] Directive 1999/93/EC of 13 December 1999 on a Community Framework for Electronic Signatures (hereinafter "Electronic Signatures Directive"). A copy of the Electronic Signatures Directive is available at www.europa.eu.int/information_society/topics/ebusiness/ecommerce/8epolicy_elaw/law_ecommerce/legal/digital/index_en.htm.

[17] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market (hereinafter "Electronic Commerce Directive"); available at www.europa.eu.int/ISPO/ecommerce/legal/documents/2000_31ec/2000_31ec_en.pdf.

[18] The United Nations Commission on International Trade Law (UNCITRAL) was established by the General Assembly in 1966 (Resolution 2205 (XXI)) as the vehicle by which the United Nations could play an active role in reducing or removing disparities in national laws governing international trade that created obstacles to the flow of trade. Its general mandate is to further the progressive harmonization and unification of the law of international trade, and it has come to be the core legal body of the United Nations system in the field of international trade law. UNCITRAL is composed of 36 member states selected by the General Assembly so as to be representative of the

work on its Model Law on Electronic Commerce[19] in 1996, and finalized and approved its Model Law on Electronic Signatures in 2001.[20] These model laws have served as the basis for legislation enacted in several countries.

Each of these laws (and many others) authorize most transactions[21] to be conducted in electronic form.[22] They effectively sweep away concerns regarding legal requirements for paper documents and ink signatures, as well as inconsistent legal requirements for enforceable electronic transactions,[23] and permit electronic commerce to proceed on a substantially uniform legal basis.

To remove the primary barriers to the use of electronic transactions, these statutes typically provide that the electronic records and electronic signatures that compromise the transactions cannot be denied legal effectiveness solely on the ground that they are in electronic form. Thus, for example, E-SIGN simply states that, notwithstanding any other rule of law, "a signature, contract, or other record relating to [a] transaction . . . may not be denied legal effect, validity, or enforceability solely because it is in electronic form."[24] Likewise, UETA provides that "a record or signature may not be denied legal effect or enforceability solely because it is in electronic form."[25] 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."[26] Similarly, the European Union Electronic Signature Directive requires member states to "ensure that an electronic signature is not denied legal effectiveness . . . solely on the grounds that it is in electronic form … ."[27] The impact of these simple provisions is important, because it prohibits a court from holding that covered

---

world's various geographic regions and its principle economic and legal systems. Further information, as well as a list of ongoing and completed projects may be found at www.uncitral.org.

[19] See United Nations, UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, available at www.uncitral.org/english/texts/electcom/ecommerceindex.htm

[20] See United Nations, UNCITRAL Model Law on Electronic Signatures 2001 www.uncitral.org/english/texts/electcom/ml-electsig-e.pdf.

[21] 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, 15 U.S.C. § 7006(13). UETA 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." UETA § 2(16).

[22] E-SIGN, 15 U.S.C. § 7001(a); UETA § 7.

[23] See Thomas J. Smedinghoff and Ruth Hill Bro, "Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce," The John Marshall Journal of Computer and Information Law, Vol. XVII, No. 3, Spring 1999 at 723. A copy of this article is available at www.bmck.com/moveart.doc.

[24] E-SIGN, 15 U.S.C. § 7001(a).

[25] UETA § 7(a).

[26] UETA §§ 7(c) and 7(d).

[27] Electronic Signature Directive, Article 5(2).

transactions are unenforceable solely because of the fact that they are conducted in electronic form.

It is important to keep in mind, however, that legislation providing for the legal recognition of electronic transactions does not in any way waive the fundamental requirements set forth in the substantive law governing the transaction. For example, although e-commerce legislation gives legal recognition to electronic contracts, the parties must still satisfy the requirements for a contract, including offer, acceptance, the inclusion of certain minimum terms, etc. E-commerce legislation simply ensures that transactions previously done on paper can now be done electronically.

Legislation authorizing the use of electronic records and electronic signatures generally applies to most business, commercial (including consumer), and governmental transactions. However, there are a variety of exceptions to the scope of transactions they authorize in electronic form. For example, in the U.S., transactions governed by the following laws, or the use of the following documents, are expressly excluded from the scope of E-SIGN, UETA, or both:

- All articles of the UCC, other than Sections 1-107 and 1-206, and Articles 2 and 2A;[28]
- 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.[29]

It is worth noting, however, that such e-commerce enabling legislation typically does not 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.

---

[28] This means, for example, that transactions governed by UCC Articles 3 (negotiable instruments), 4 (bank deposits and collections), 4A (funds transfers), 5 (letters of credit), 6 (bulk sales), 7 (warehouse receipts, bills of lading and other documents of title), 8 (investment securities), and 9 (secured transactions; sales of accounts and chattel paper) are not covered by either E-SIGN or UETA. Note, however, that some of these articles already include express provisions for electronic transactions (such as Article 4A and Article 9).

[29] See, E-SIGN, 15 U.S.C. § 7003, and UETA § 3(b) for a complete list of exceptions.

1.3 E-SIGN or UETA – Which One Applies?

The relationship between E-SIGN and UETA has been the source of some confusion. UETA was finalized in July 1999 as a uniform law designed to be enacted by each of the states. A year later, however, Congress passed E-SIGN in an attempt to accomplish a similar purpose at the national level. Both statutes are similar, although there are a number of substantive differences, such as the comprehensive consumer notice and consent requirements that appear in the E-SIGN legislation.

E-SIGN is a sweeping federal statute that applies to all transactions "in or affecting interstate or foreign commerce."[30] E-SIGN thus preempts all inconsistent state law.[31] However, E-SIGN contains a provision granting the states authority to "modify, limit, or supercede the provisions of Section 101" of E-SIGN.[32] States may exercise this authority in one of two ways:

- By adopting the official version of UETA without any changes, or
- By adopting a law that specifies "alternative procedures or requirements for the use or acceptance (or both) of electronic records or electronic signatures" provided that such alternate procedures are consistent with E-SIGN and do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for electronic records or signatures.[33]

This provision creates a situation where E-SIGN applies to some electronic transactions and UETA applies to others, depending in large part on law enacted in the state whose law will govern the transaction. Moreover, because most of the states that have enacted UETA have made some changes to the official form adopted by NCCUSL, there is a further question as to whether these enactments of UETA supercede E-SIGN.

This article will not attempt to address the complex federal preemption issues involved here.[34] However, for purposes of analyzing legal requirements for electronic transactions, two points should be noted. First, there is a significant similarity in the approach taken by both E-SIGN and UETA. Major differences, such as the consumer consent provisions in E-SIGN, are noted. Second, for many parties entering into electronic transactions on a nationwide basis, the preemption issue may be moot, as it may ultimately be necessary to comply with the requirements of both statutes in order to ensure the enforceability of transactions in all relevant jurisdictions.

---

[30] E-SIGN 15 U.S.C. § 7001.

[31] See Smedinghoff and Bro, supra note 23, for discussion of the various approaches taken by state electronic signature legislation prior to the enactment of E-SIGN.

[32] E-SIGN, 15 U.S.C. § 7002(a).

[33] E-SIGN, 15 U.S.C. § 7002(a).

[34] For an excellent discussion of this issue, see Robert A. Wittie and Jane K. Winn, "Electronic Records and Signatures Under the Federal E-SIGN Legislation and the UETA," The Business Lawyer, Vol. 56 No. 1, November 2000, at 293.

2. Key Questions for Electronic Transactions

With legislation in place that authorizes the use of electronic records and electronic signatures in lieu of paper records and handwritten signatures, the next question becomes: what are the legal requirements must be satisfied in order to create valid and enforceable electronic transactions. Although existing laws diverge on this issue, there are three fundamental questions to consider:

- **What requirements are imposed by e-transaction laws?** Assuming that, under applicable law, a particular transaction (e.g., contract, promissory note, letter of credit, etc.) can be done in electronic form, what additional requirements must be satisfied so that the electronic version of the transaction will be legally enforceable?
- **Do the parties trust the message?** Even if the legal requirements are satisfied, are the parties to the transaction sufficiently comfortable with the authenticity and integrity of the communications and 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?[35]
- **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, such as rules regarding the time an electronic message is considered sent, the time the message is considered received, the place the message is considered sent from and received at, etc?

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

3. Requirements Imposed by E-Transaction Laws

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

- **Notice and Consent**. Have the parties consented to conduct this transaction in electronic form? Have the requisite notices been provided?
- **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 electronic records comprising the transaction available to all parties?

---

[35] 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. 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.

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

The following sections will summarize each of these issues.

3.1 Notice and Consent Requirements

Because electronic transactions are fundamentally different than more traditional ways of doing business, and because they present enhanced risks in a variety of areas, some e-transaction legislation expressly requires that the parties consent to enter into a transaction electronically before it will be considered enforceable. In the U.S., this concept appears in both E-SIGN and in UETA.

As a starting point, both E-SIGN and UETA make clear that while they "authorize" electronic transactions, nothing in either statue requires a party to conduct any transaction in electronic form.[36] This preserves the right of a party[37] to refuse to enter into any transaction in electronic form.[38]

UETA goes further, however, as the statute is premised on the requirement of consent. Thus, the benefits of the statute will not apply unless the parties have "*agreed* to conduct transactions by electronic means."[39] Whether the parties have agreed to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties conduct,[40] 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, but that is not necessary. 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.

The UETA consent provisions apply to all transactions within its scope, both business and consumer. E-SIGN, on the other hand, contains an extensive disclosure and consent provision, but only for certain limited types of consumer transactions. It applies only when a

---

[36] E-SIGN, 15 U.S.C. § 7001(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 §s 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.")

[37] Other than governmental agencies. See E-SIGN, 15 U.S.C. § 7001(b)(2).

[38] Of course, there is nothing to stop a business from announcing to its customers or trading partners that it will only do business with them via electronic transactions.

[39] UETA § 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, 15 U.S.C. § 7001 (c), discussed below.

[40] UETA § 5(b), and comment 3. Some state enactments of UETA (e.g., California), require such consent to be in electronic form.

statute, regulation, or other rule of law requires that information relating to a transaction be provided or made available to a consumer in writing.[41] 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 receive an electronic record in lieu of a paper record, provides such consent electronically, and does so in a manner that reasonably demonstrates that he or she can access the electronic information in the form that will be used.[42]

Moreover, prior to consenting, the consumer must be provided with a clear and conspicuous notice that informs the consumer of:

- His/her option to have the information provided on paper;
- Whether the consent to receive the information in electronic form 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;
- The procedures the consumer must use to update information needed to contact the consumer electronically;
- After consent, how he/she may obtain a paper copy of the electronic record, and the fee therefore;
- The hardware and software requirements for access and retention of the electronic records,
- His/her option to withdraw such consent, and the procedures the consumer must use to withdraw consent; and
- The conditions, consequences, and fees of withdrawing such consent.[43]

The European Union Electronic Commerce Directive takes a slightly different approach that appears to be intended to achieve the same goal. It does not require consent of the parties, but instead requires that information society services (e.g., sellers of goods online) provide a variety of information to the other party regarding the transaction. Required information includes a comprehensive and unambiguous statement as to the technical steps to follow to conclude the contract, whether or not the concluded contract will be filed by the service provider and where it will be accessible, the technical means for identifying and correcting input errors

[41] E-SIGN, 15 U.S.C. § 7001(c). Examples might include laws requiring written disclosure of interest rate charges in consumer loan transactions, or laws requiring that consumers be provided with periodic written statements of account.

[42] E-SIGN, 15 U.S.C. §§ 7001(c)(1)(A) and 7001(c)(1)(C)(ii). It is not clear from the statute whether this obligation to "reasonably demonstrate" ability to access the information 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.

[43] E-SIGN, 15 U.S.C. § 7001(c) (1)(B).

prior to the placing of the order, and the languages offered for the conclusion of the contract.[44] The service provider is also obligated to acknowledge receipt of the purchaser's order without undue delay and by electronic means, and is required to make available to the purchaser appropriate, effective, and accessible technical means allowing him to identify and correct input errors prior to the placing of the order.[45]

3.2 Signature Requirements

Signatures can serve a variety of purposes in a transaction. The primary uses for a signature can be summarized as follows:

- **Expression of Intent** – A signature evidences the signer's intent with respect to the document signed. 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 a contract, the approval of a subordinate's request for funding of a project, authorization to a bank to transfer funds, confirmation that the 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.
- **Satisfaction of Legal Requirements** – A signature is often used to satisfy a 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.
- **Security** - Signatures often function as a security device. That is, signatures can be used (1) to authenticate a document (i.e., to identify the signer and indicate that such person is the source of, or has approved, the document), and/or (2) to ensure the integrity of the document (i.e., to ensure that the document has not been altered since it was signed).[46]

Traditionally, under U.S. law, any *symbol* that is made with the *intent* to sign a document can qualify as a legally valid signature. 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

[44] Electronic Commerce Directive, Article 10(1).

[45] Electronic Commerce Directive, Article 11(1) and 11(2).

[46] It is for this reason, for example, that parties to a multi-page contract will sometimes initial each page of the contract. In the electronic environment, certain types of signatures (e.g., cryptographically-created digital signatures) can play an important role in verifying the integrity of the entire document.

party with present *intention* to authenticate a writing."[47] The primary focus is on the "intention to authenticate" a document, which distinguishes a signature from an autograph.

Both E-SIGN and UETA extend this basic approach to the concept of an electronic signature. To be enforceable under U.S. law, they require that an electronic signature possess three elements:[48]

- A sound, symbol, or process,
- Attached to or logically associated with an electronic record,[49] and
- Made with the intent to sign the electronic record.[50]

Electronic signatures that meet these requirements are considered legally enforceable as substitutes for handwritten signatures for most transactions in the U.S.[51]

The definition of electronic signature recognizes that there are many different methods by which one can "sign" an electronic record. Although electronic signatures, by their nature, are represented digitally (i.e., as a series of ones and zeroes) they can take many forms, and can be created by many different technologies. Examples of electronic signatures (that qualify under E-SIGN and UETA) include:

- A name typed at the end of an e-mail message by the sender;[52]
- A digitized image of a handwritten signature that is attached to an electronic document (sometimes created via a biometrics-based technology called signature dynamics[53]);

---

[47] U.C.C. Article 1, § 1-201(39) (1999).

[48] E-SIGN, 15 U.S.C. § 7006(5) and UETA § 2(8) (definitions of "electronic signature").

[49] 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.

[50] 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.

[51] See UETA §s 2(8) and 7(d) and E-SIGN, 15 U.S.C. § 7001(a) and 7006(5). The European Union Electronic Signature Directive also uses a similar definition of an electronic signature. Under the Directive, an electronic signature must also possess three elements: (1) data in electronic form, (2) attached to or logically associated with other electronic data, and (3) which serves as a method of authentication. Electronic Signature Directive, Article 2(1).

[52] Shattuck v. Klotzbach, 2001 Mass. Super. LEXIS 642 (December 11, 2001)

[53] Signature Dynamics' involves measuring the way a person writes his or her signature by hand on a flat surface such as speed, pressure, angle, size, etc., and binding those measurements to a message.

- 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);[54]
- 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).[55]

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.

There is a big difference, however, between an electronic signature that merely satisfies the requirements of E-SIGN and UETA, and a trustworthy electronic signature. As a consequence, parties who desire to engage in electronic transactions may find that merely using a legally compliant electronic signature is not sufficient. As discussed above, clicking a mouse on an "I accept" button or typing a name on an e-mail message both qualify as legally enforceable signatures. But by themselves, they offer no evidence as to "who" clicked the mouse or typed the name that appears on the electronic document. Thus, to say that they are legally enforceable may be somewhat illusory, as a party's ability to authenticate a signature or use it to verify the integrity of a document may be very limited at best. 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.

---

[54] 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 § 2, comment 7. It is not clear whether the "process" of clicking a mouse on an I Accept button will satisfy the definition of a signature in the EU Electronic Signature Directive, as such definition requires that the signature constitutes "data in electronic form". See EU Directive at Article 2(1).

[55] 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. 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. 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).

For electronic transactions, these security-related 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/signer and the integrity of the document becomes pivotal. Thus, while removing the so-called signature "barrier" to electronic transactions may have been an important legislative step, it is also important to recognize that an electronic signature, by itself, may not provide the security that a unique handwritten signature is thought to carry on a paper-based transaction. This need for security – for trusting the transaction – is addressed in Section 4 below.

3.3 Record Accessibility Requirements

Another key requirement for the enforceability of electronic transactions is that the documents that comprise the transaction be communicated in a form that can be retained and accurately reproduced by the receiving party. In the U.S., 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."[56] 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."[57]

The European Union Electronic Commerce Directive contains a similar requirement governing contracts with information society services (e.g., for the sale of goods). Under the Directive, contract terms and general conditions "must be made available in a way that allows him to store and reproduce them."[58]

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

3.4 Record Retention Requirements

An essential element for the enforceability of all 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., regulations governing the insurance, securities, and banking industries, etc.), as well as the requirements of government agencies, such as the IRS. For

[56] E-SIGN, 15 U.S.C. § 7001(e).

[57] UETA § 8(c).

[58] Directive 2000/31/EC (Electronic Commerce Directive), Article 10(3).

electronic transactions, the issue 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, storage of an electronic record will satisfy legal record retention requirements if the stored copy of the electronic record:

- Accurately reflects the information set forth in the record[59] and;
- Remains accessible for later reference.[60]

With respect to evidentiary rules, both E-SIGN and UETA also provide that if a rule of evidence or other rule of law requires a record relating to a transaction to be provided or retained in its original form, this obligation is satisfied by meeting the accuracy and accessibility requirements listed above.[61] These provisions also make clear that records can be kept in electronic-only form. Moreover, it provides a great deal of flexibility to the parties in terms of how they store the records, when and whether they migrate the records to new media, and meeting applicable evidentiary requirements.

4. Security -- Is the Transaction Trustworthy?[62]

Beyond compliance with the statutory requirements for legal enforceability, the primary concern of parties to an electronic transaction is the pivotal question of "trust." To say that an electronic transaction complies with legal requirements is one thing. To have a sufficient degree of trust in an electronic transaction such that one is willing to ship product, transfer funds, or enter into a binding contractual commitment in real time is something else.

The loss of trust can have a significant impact. For example, on August 26, 2002, the Reuters News Agency reported that large South Korean investors had stopped trading stocks online as a result of a disclosure from Daewoo Securities, Korea's fourth largest brokerage, that an unauthorized person had used one of its client accounts to buy almost $22 million of shares. The matter involved the apparently unauthorized purchase of 5 million shares in Delta Information and Communications over a period of 90 seconds.[63] The loss of trust was, of course,

---

[59] Both E-SIGN and UETA make clear that this requirement does not extend to information whose sole purpose is to enable the contract or other record to be sent, communicated, or received. E-SIGN, 15 U.S.C. § 7001(d)(2); UETA § 12(b).

[60] UETA § 12(a); E-SIGN, 15 U.S.C. §7001(d). E-SIGN requires that the stored electronic record 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.

[61] E-SIGN 15 U.S.C. § 7001(d)(3); UETA § 12(d).

[62] Portions of this section are adapted from Thomas J. Smedinghoff, Ed., Online Law, Chapter 3, by Lorijean G. Oei (1996).

[63] "Daewoo Securities Hit by Online Trade Fraud," Reuters News Agency, August 26, 2002, as reported on Yahoo at http://asia.tech.yahoo.com/020826/reuters/asia-122181-tech.html.

immediate. According to the article, one of Korea's biggest institutional investors was quoted as saying "starting today, we started to stop online trading for the time being because of the security risks."

4.1 The Requirements for Trust

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, each of the transacting parties must have some level of trust before they will be willing to proceed with the transaction. But trust has different components. Trusting one's business partners has always been important (e.g., Are they reputable and creditworthy? Will they perform as promised?). But in today's e-business environment, companies also need to trust *the transaction itself.*

What does trusting the transaction mean? When vital business transactions depend on computer and network availability, the parties need to know that these will work properly and without interruption. When remote communications replace personal contact or a trusted medium such as the mail, the parties need to verify each other's identity. When easily copied and altered electronic records replace signed paper documents, the parties need assurance that these records are authentic and unaltered. And when sensitive data is stored electronically, the parties need assurances that the data is protected and accessible.[64]

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.[65]

Ensuring that an electronic transaction is trustworthy, from a legal perspective, requires consideration of four issues: authenticity, integrity, confidentiality, and nonrepudiation.

---

[64] Of course, the requirement for such trust is a relative concept that 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. The bookstore 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 (e.g., $20) is relatively low. On the other hand, shipping $200,000 worth of product based on electronic message may require a much higher level of trust. 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. At a minimum, the risk of a fraudulent message must be acceptable given the nature and size of the transaction.

[65] Commission of the European Communities, A European Initiative in Electronic Commerce, COM (97) 157 final, Apr. 16, 1997); available at www.cordis.lu/esprit/src/ecomcom.htm.

(a) Authenticity — Who Sent the Message?

Authenticity is concerned with the *source or origin* of a document or message.[66] Who created or signed the document? Who sent the message? Is it genuine or a forgery?

A party entering into a 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.[67]

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.[68]

A signature *can* be used to authenticate the source of a document. This works very well with handwritten signatures on paper documents, as such signatures can usually be related to a specific person, through handwriting analysis if necessary. But, most legally recognized electronic signatures do not perform this function, or provide such a weak level of authentication that they have little or no evidentiary value for that purpose.[69] For example, while E-SIGN and UETA both recognize that typing one's name, clicking a mouse, or almost any other sound or symbol, can constitute a valid electronic signature, it is readily apparent that such signatures, by themselves, do little to authenticate the source of a document. The ultimate question – who typed the name, or who clicked the mouse – often remains unanswered.

Some electronic transaction legislation attempts to address this problem by requiring that an electronic signature contain both information from which the signer can be identified and a level of security designed to ensure that the signature was in fact made by the person identified.[70]

---

[66] See FED. R. EVID. 901(a) (1995).

[67] See U.C.C. §§ 4A-202, 4A-203 & cmt. (1998). § 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. If the bank verifies the payment order by using a commercially reasonable security procedure, the customer will 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).

[68] 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).

[69] Some forms of electronic signature, such as the cryptographically created digital signature, if properly implemented, can provide strong authentication as to the source of the signature. Certain biometric techniques can also achieve a similar result.

[70] The UNCITRAL Model Law on Electronic Signatures, for example, requires that a signature identify the signer and that it be "as reliable as was appropriate for the purpose" for which the message was generated or

However, most electronic transaction legislation (including E-SIGN and UETA) recognizes the validity of electronic signatures that are, in many respects, the legal equivalent of signing a paper contract with an "X". They leave unanswered the question of proving up the identity of the signer.

(b) Integrity — Has the Document 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 concern regarding integrity flows from the fact that electronic documents are easily altered in a manner that is not detectable. Moreover, because every copy of an electronic document is a perfect reproduction, there is no such thing as an original electronic document. Thus, unlike paper documents, electronic records come with no inherent attributes of integrity.

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 contractor who wants to solicit bids from subcontractors and submit its proposal to the government online. The 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 a 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.[71]

A signature *can* be used to verify the integrity of a document. This works reasonably well with paper documents where a handwritten signature (or initials) placed at the bottom of each page is often a reasonably reliable way of preventing undetected alterations. But most legally recognized electronic signatures do not perform this function. Clicking a mouse or typing one's name on an easily altered electronic document is no guarantee of document integrity. Typically, the use of cryptographic algorithms, often coupled with digital signatures, is the only way to detect alteration in an electronic document.

(c) Confidentiality

Confidentiality is concerned with controlling the disclosure of information. It involves: (1) protecting information so that unauthorized persons cannot have access to it, and/or (2) protecting information so that even if unauthorized access is obtained, the information is unreadable (e.g., by encrypting the information).

---

communicated. By including these elements in the definition of an electronic signature, this Model Law seeks to require a minimum level of security before such signature will be considered legally enforceable. UNCITRAL Model Law on Electronic Signatures, Article 2(a) and Article 6(1).

[71] See, e.g., Victory Med. Hosp. v. Rice, 493 N.E.2d 117 (Ill. App. Ct. 1986).

Confidentiality may not be an issue in all situations. In some cases, however, it is critical. Maintaining a competitive advantage, or other business reasons, may require that certain information be kept confidential. In addition, statutes and regulations designed to protect the privacy of personally identifiable information typically require that such information be kept confidential, except when used in a manner authorized by law.[72] Likewise, confidentiality may be necessary to protect a property right in information, such as a trade secret right. Information can only qualify as a trade secret if it is not generally known, and reasonable security precautions are taken to maintain secrecy.[73] In addition, confidentiality may be necessary to comply with certain legal obligations, such as an obligation not to disclose the contents of attorney-client communications,[74] or obligations arising as a result of contractual commitments. Confidentiality may also be important for preventing access to and use of information that can cause harm to the owner of the information, such as credit card or bank account numbers, social security numbers.

(d) Nonrepudiation — Can the Message Be Proved in Court?

Nonrepudiation flows from authenticity and integrity. It is the ability to prove that the originator of a document in an electronic transaction intended to be bound by the terms of the document – i.e., to hold the sender to his communication in the event of a dispute.[75] A person's willingness to rely on a communication, contract, or funds transfer request is typically contingent upon having some level of comfort that he 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 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.[76]

4.2 The Challenge of the Electronic Environment

With paper-based transactions, a party can rely on numerous indicators of trust to ensure the authenticity, integrity, confidentiality, and nonrepudiability of a document. These include using paper (sometimes with letterhead, watermarks, colored backgrounds, or other indicia of reliability) to which the message is affixed and not easily altered, handwritten ink

---

[72] See, e.g., regulations governing "Standards for Privacy of Individually Identifiable Health Information," 45 C.F.R. Parts 160 and 164, August 14, 2002.

[73] See, e.g., 1 Melvin F. Jager, Trade Secrets Law §§ 3.04[6],[7], 5.05[2] (1995).

[74] See, e.g., Cal. Evid. Code §§ 950 et seq. (1995); American Bar Association, Model Rules of Professional Conduct Rule 1.6 (1992).

[75] 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. 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." Id. at § 1.20.

[76] See generally, John Browning, Follow the Money -- A New Stock Market Arises on the Internet, SCI. AM. 31 (July 1995), and "Daewoo Securities Hit by Online Trade Fraud, "Reuters News Agency, August 26, 2002, as reported on Yahoo at http://asia.tech.yahoo.com/020826/reuters/asia-122181-tech.html.

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 the use of electronic documents and electronic communications conducted remotely over the Internet, 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 that can be easily copied and modified without detection.

Thus, moving transactions to an electronic environment 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, especially for significant transactions. Second, this lack of reliability can make proving up one's case in court difficult at best. For example, if the defendant denies making the "signature" that is appended to an electronic document, it may be virtually impossible for the plaintiff to prove the authenticity of that electronic signature, absent additional evidence.

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).

4.3 The Law and Trust In Electronic Transactions

Establishing trust in an electronic transaction requires security – specifically, the use of security procedures[77] designed to ensure the authenticity, integrity, confidentiality, and/or nonrepudiation of electronic documents and messages. There are a number of security procedures that can be used to assist in establishing trust for electronic communications. These include:

- Algorithms or codes[78]
- Cryptography and digital signatures
- Identifying words or numbers
- Replies and acknowledgments
- Repeat-back acknowledgements
- Using an automated process or system[79]

---

[77] 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. UETA § 2(14), and UCC Article 4A § 201.

[78] See generally, Warick Ford and Michael Baum, Secure Electronic Commerce (1997).

[79] See Fed. R. Evid. 901(b)(9)(1995).

- Date/time stamping
- Using trusted third parties to retain copies of electronic communications
- Encryption.

Regardless of the security measures employed, it is important to note that, increasingly, the law is recognizing the importance of security procedures in determining the enforceability of an electronic transaction and the allocation of risk in the event of a loss. The first formal recognition of the legal effect of security procedures occurred in 1989 with the approval of Article 4A of the UCC.[80]

Article 4A addresses the electronic transfer of funds by wire.[81] 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, 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.[82] 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 to ensure the authenticity and integrity of the message. Thus, under Article 4A, an electronic message purporting to be from a bank's customer that instructs the 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 the authenticity and integrity of the order is "verified" pursuant to a "commercially reasonable" security procedure, regardless whether the order was actually authorized by the customer. The bottom line is that Article 4A adopts "security procedures" rather than "signatures" as the basis for verifying electronic transactions and apportioning liability.

Since the advent of UCC Article 4A, the law is starting to recognize that security has a key role to play in electronic transactions. Approaches vary, however, and currently, electronic transactions statutes fall into the falling categories with respect to security:

- **Security not addressed**. Many statutes say nothing at all with regard to the role of security. They merely authorize the use of electronic records and signatures in lieu of paper records and signatures (and in some case provide for other transactional requirements, such as consent), but say nothing about, or give no legal effect to, the use of security procedures. This is the approach taken by E-SIGN and UETA.
- **Security as a precondition to enforceability**. Some statutes *require* the use of security, at some level, before the transaction (or some aspect of it) will be legally enforceable. The UNCITRAL Model Law on Electronic Signatures, for example, requires an element of "reliability" – i.e., that electronic signatures be as reliable as appropriate for the circumstances, before the electronic signature will be considered valid. Likewise, the electronic signature must be capable of identifying the signer,

[80] See U.C.C. Art. 4A, Funds Transfers (1989). Article 4A has since been adopted in all 50 states.

[81] U.C.C. Art. 4A, Prefatory Note (1990).

[82] U.C.C. § 4A-203 Official Comment.

another aspect of security. Many of the electronic signature statutes enacted by the various states in the U.S. also took a similar approach (although they are largely preempted by E-SIGN now).[83]

- **Incentives for security – legal presumptions**. A number of 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.[84] 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. Thus, these statutes, while not literally requiring security as a precondition to the enforceability of electronic transactions, provide incentives for security by providing a legal benefit (i.e., a presumption) to those who use security to assist them in ensuring that the transaction will be enforceable.

- **Security as a risk allocation device**. Finally, some legislation uses the presence or absence of security as a risk allocation device. UETA, for example, in some cases allocates the risk of loss for errors or mistakes to the party that failed to implement agreed-upon security procedures. Likewise, UCC Article 4A allocates the risk of loss for fraudulent electronic payment orders based on the presence or absence of an agreed-upon security procedure.

---

[83] Several states enacted electronic signature statutes that adopted security requirements from a decision of the U.S. Comptroller General. *See* U.S. Comptroller General, *Matter of National Institute of Standards and Technology" Use of Electronic Data Interchange Technology to Create Valid Obligations*, 71 Comp. Gen. 109 (1991); (Dec. 13, 1991). Under those statutes an electronic signature is legally effective as a signature only if it is: (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. This approach requires attributes of security as a precondition to the validity of the signature itself, something not required for paper-based signatures. States with statutes adopting this approach include ALASKA STAT. § 09.25.510 (Michie 1999) (applying generally to all communications); CAL. GOV'T CODE § 16.5 (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 (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. STAT. ANN. § 369.020 (Banks-Baldwin 1999) (applying generally to all kinds of communications); MD. CODE. ANN. STATE GOV'T § 8-504 (1998) (limiting application to any communications among governmental entities); NEB. REV. STAT. § 86-1701 (1998) (applying generally to all communications); N.H. REV. STAT. ANN. § 294-D:4 (1999) (limiting application to communications between the state and any agency or instrumentality of the state); N.C. GEN. STAT. § 66-58.1 (1999) (limiting application to filings with public agencies); OKLA. STAT. ANN. TIT. 15 § 965 (West 1999) (applying generally to all communications); R.I. GEN. LAWS § 42-127-4 (1998) (limiting application to transactions between public agencies).

[84] 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.

A good example of legislation that provides for legal presumptions is the Illinois Electronic Commerce Security Act, which creates a technology neutral class of trustworthy signatures called "secure electronic signatures."[85] While all electronic signatures are enforceable under this Act, 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.[86] This approach was followed in the European Union Electronic Signature Directive. Under this Directive, while electronic signatures cannot be denied enforceability solely because they are in electronic form, a more secure form of electronic signatures – referred to as "advance electronic signatures" – are presumed to satisfy legal requirements for signatures, and are presumed admissible as evidence in legal proceedings.[87]

Technology-specific statutes that confer similar legal presumptions on certain cryptographically created "digital signatures" have been enacted in Minnesota, Missouri, Utah, and Washington.[88] 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 that voluntarily elect to be licensed by the State.[89] 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.[90]

There is, of course, a great deal of debate over whether, or how, the law should address the role of security in electronic transactions. But regardless of the outcome of that public policy debate, there can be do denying that security is an ever-increasing concern for electronic transactions. And even where it is not given special recognition in legislation, it will ultimately become important in the evidentiary process in the event of a dispute. Whether an electronic record is admissible, or the weight that it will be given by the trier of fact, will ultimately depend on the ability of the proponent of the electronic document to establish its authenticity and integrity – factors which hinge upon the sufficiency of the security measures employed under the circumstances.

---

[85] 5 ILL. COMP. STAT. 175/10-110 (1998). This Act also defines a class of secure electronic records. Id. at 175/10-110. See generally, 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.

[86] 5 ILL. COMP. STAT. 175/10-120.

[87] Electronic Signature Directive, Article5(1).

[88] See MINN. STAT. ANN. § 325K.20 (West 1998); MO ANN. STAT. § 28.677 (West 1998); UTAH CODE ANN. § 46-3-101 (1998); WASH. REV. CODE § 19/34/900 (West 1998).

[89] 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.

[90] 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.

5. What Rules Govern the Transaction?

Finally, for any electronic transaction, the parties need to know the rules that govern their use of the electronic medium for communication and storage. And these rules can differ significantly from those that govern transactions documented on paper. Questions to be considered, for example, include rules regarding the time and place of sending and receipt of electronic documents, the notarization of electronic documents, and the effect of errors introduced into the communication process.

Unfortunately, most electronic transaction statutes enacted to date say little or 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 these issues.

5.1 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 an 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 court held that a fax transmission was not effective notice because, while it was started before the deadline passed, it was not completed until afterwards.[91] 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 where both parties are on AOL).[92] 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 provided further that it is in a form capable of being processed by that system.[93]

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

---

[91] 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).

[92] UETA § 15(3).

[93] UETA § 15(a)(1) and 15(a)(2).

processed by that system.[94] 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.

5.2 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.

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.[95] 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.[96] E-SIGN does not address this issue.

5.3 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.[97] In theory, the same rule should apply to electronic contracts, although there is very little law on the subject. There are fundamental provisions in E-SIGN, UETA, and the UNCITRAL Model Law on Electronic Commerce that support the validity of electronic contracts, but little more than that. In part due to this fact, in 2001 UNCITRAL began a project to develop an international convention on electronic contracting.[98] Similarly, in the United States, an industry group known as the Electronic Financial Services Counsel has initiated a Standards and Procedures for Electronic Records and Signatures (SpeRS) project to address these issues and develop appropriate standards.[99]

E-SIGN provides that "a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation."[100] Similarly, UETA provides that "a contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation."[101] Finally, the UNCITRAL Model Law on Electronic Commerce goes a bit further by providing both that "an offer and the acceptance of an offer may be expressed by means of data messages", and

---

[94] UETA § 15(b).

[95] UETA § 15(d).

[96] UETA § 15(d).

[97] UCC 2-204.

[98] See www.uncitral.org/en-index.html.

[99] See www.spers.org.

[100] E-SIGN, § 101(a)(2).

[101] UETA, § 7(b).

"where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose."[102]

As a general rule, 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.[103] 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."[104] 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.[105] 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.[106] 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."[107] Thus, if the parties have regularly corresponded in the past by e-mail, an e-mail acceptance sent to the offeror's 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.

5.4 Automated transactions

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

A computer can certainly 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.[108]

---

[102] UNCITRAL Model Law on Electronic Commerce, Article 11(1).

[103] Of course, there can be questions about the reliability of electronic communications, which may make it more difficult to introduce evidence in court. Security issues are discussed above in Section 4.

[104] UCC 2-206(1)(a).

[105] 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.

[106] 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).

[107] UETA § 15(b)(1).

[108] State Farm Mutual Auto. Ins. Co v. Brockhurst, 453 F.2d 533 (10th Cir. 1972)

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.[109]

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.[110] 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.[111]

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.[112]

Both E-SIGN and UETA 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 bound.[113] Likewise, 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.[114] In addition, UETA recognizes that a contract may be formed by the interaction of an electronic agent and an individual.[115]

---

[109] 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.

[110] 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.

[111] UETA § 15(f).

[112] See E-SIGN § 106(3); UETA § (2)(6).

[113] E-SIGN § 101(h).

[114] UETA § 14(1).

[115] UETA § 14(2).

5.5 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 applied the security procedure, the conforming party may avoid the effect of the changed or erroneous record.[116] 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.[117]

5.6 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.[118] 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.

5.7 Party Autonomy

One final point is worth noting. With the law in a state of flux, a common approach for parties regularly engaged in electronic transactions between themselves is to simply enter into their own contract to decide the rules that will govern their online conduct. This concept of party autonomy – i.e., the right of the parties to agree between themselves as to the rules that govern their transactions – has been a core premise of the U.S. government position regarding electronic commerce.

---

[116] UETA § 10(1).

[117] UETA § 10(2).

[118] E-SIGN § 101(g); UETA § 11.

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.[119] E-SIGN, however, like most other legislation, is simply silent on the subject of party autonomy. And some legislation (such as consumer protection legislation) actually prohibits variation of its terms by agreement.

In the absence of laws that prohibit changes of the rules by agreement of the parties,[120] the courts generally uphold such agreements.[121] The Supreme Court stated "[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."[122] The Court did note, however, "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."[123]

Thus, some contracts that purport to alter existing legal rules have been held unenforceable. In one case, for example, the court refused to enforce an agreement that only certain types of appraisals would be admissible, on the ground that such a provision "purported to totally preempt the court from its consideration of legally competent evidence."[124] In another case, the court held that a licensee could dispute a contractual recital that trademark infringement was conclusive evidence of irreparable injury.[125] 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."[126] Finally, some courts have upheld provisions in insurance policies that alter the legal presumption of death after absence for seven years, although many other courts refuse to enforce such agreements.[127]

---

[119] UETA § 5(d).

[120] For example, UETA § 5(c) provides that "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."

[121] For example, 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)).

[122] United States v. Mezzanatto, 513 U.S. 196, 115 S. Ct. 797, 803 (1995), citing 21 C. Wright & K. Graham, Federal Practice and Procedure § 5039, pp. 207-208 (1977).

[123] Mezzanatto, 513 U.S. 196, 115 S. Ct. at 803.

[124] Cronk v. State, 420 N.Y. S.2d 113 (N.Y. Ct. Cl. 1979).

[125] Oleg Cassini, Inc. v. Couture Coordinates, Inc., 297 F. Supp. 821, 833 (S.D.N.Y. 1969).

[126] Transamerica Insurance Co. v. Bloomfield, 55 Or. App. 31, 637 P.2d 176, 180 (1981).

[127] See Williston on Contracts (4th ed.), Vol. 7, § 15.13, pp. 274-275 (1997).

In most cases, however, contracts between trading partners (especially in a business-to-business context) that establish rules for electronic transactions where none previously existed, or that alter existing rules, will be enforced. Until the law governing electronic transactions evolves further, this is often the best way for the parties to ensure the enforceability and security that they require.

* * *

THOMAS J. SMEDINGHOFF is a partner with the global law firm of Baker & McKenzie and North American Coordinator of the Firm's E-Commerce Practice. His practice focuses on the legal aspects of e-business, with an emphasis on electronic transactions, security, digital signatures/PKI, and privacy issues. Mr. Smedinghoff has been actively involved in developing e-commerce legal policy both in the U.S. and globally. He chaired the Illinois Commission on Electronic Commerce and Crime, which drafted the Illinois Electronic Commerce Security Act (5 Ill. Comp. Stat. 175). He is a member of the U.S. Delegation to the United Nations Commission on International Trade Law (UNCITRAL), where he participates in the Working Group on Electronic Commerce. Mr. Smedinghoff also chairs the American Bar Association Electronic Commerce Division, is the immediate past Chair of the ABA Section of Science & Technology Law, and has served as the ABA's advisor to the National Conference of Commissioners on Uniform State Laws (NCCUSL) Drafting Committee on the Uniform Electronic Transactions Act (UETA). He is the editor and primary author of the e-commerce book titled *Online Law* (U.S. publication by Addison-Wesley, 1996, 6th printing 2000; Japanese translation and publication by Shichiken Publishing Co., Ltd., 1998; Chinese translation and publication by CS&S Electronic Press, 2002).