

The Legal Challenges of Implementing Electronic Transactions

THOMAS J. SMEDINGHOFF

ABOUT THE AUTHOR

Thomas J. Smedinghoff is a partner in the Privacy, Data Security, and Information Law Practice at the law firm of Wildman Harrold in Chicago. Mr. Smedinghoff is a member of the U.S. Delegation to the United Nations Commission on International Trade Law (UNCITRAL), where he participated in the negotiation of the United Nations Convention on the Use of Electronic Communications in International Contracts. He has also served as an American Bar Association representative to the Drafting Committee for the Uniform Electronic Transactions Act (UETA) and chair of the Illinois Commission on Electronic Commerce and Crime (1996-1998), which wrote the Illinois Electronic Commerce Security Act (5 Ill. Comp. Stat. 175). He can be reached at smedinghoff@wildman.com.

1. AUTHORIZATION—CAN THIS TRANSACTION BE DONE IN ELECTRONIC FORM?

1.1 The Primary E-Transaction Laws

1.2 The Basic Approach—Nondiscrimination and Functional Equivalence

2. ELECTRONIC REQUIREMENTS—WHAT ARE THE ELECTRONIC-SPECIFIC RULES?

2.1 Agreement to Engage in Electronic Transactions

2.2 Consumer Consent to Receive Certain Information in Electronic Form

2.3 Transaction Information Disclosure Requirements

2.4 Transaction Record Accessibility Requirements

- 2.5 Signature Requirements**
- 2.6 Method of Electronic Delivery**
- 2.7 Electronic Record Format Requirements**
- 2.8 Electronic Record Retention Requirements**
- 3. SECURITY—IS THE TRANSACTION TRUSTWORTHY?**
 - 3.1 Security Basics**
 - (a) Authentication**
 - (b) Availability of Data**
 - (c) Data Integrity**
 - 3.2 Security and the Enforceability of Electronic Transactions**
- 4. PUTTING IT ALL TOGETHER—THE CRITICAL ROLE OF “PROCESS”**
- 5. CONCLUSION**

Today more than ever, businesses face increasing pressure to conduct more and more of their transactions in electronic form. Competitive concerns, the need for increased speed and efficiency, and the benefit of significant cost savings are just some of the key motivators.

There are, of course, an endless variety of different types of transactions that could be done electronically. These include contracts governing the purchase and sale of goods, lease agreements, 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, employment applications, consent forms, delivery of documents, proxy agreements, and the like. Moving those transactions to an electronic environment, however, is often more complicated than expected.

For businesses that want to set up a process to implement any type of electronic transaction¹ on a repetitive basis, whether via a Web site, by e-mail, by traditional electronic data interchange, or even in person, a variety of fundamental issues must be addressed to ensure that the resulting process is legally valid and enforceable. Those issues can be summarized by the following three general questions:

- *Authorization—Can this transaction be done in electronic form?* Does existing law in the relevant jurisdictions allow the parties to conduct the proposed transaction in electronic form, or does existing law either prohibit doing the transaction electronically or present legal barriers that make its enforceability uncertain?
- *Electronic Requirements—What are the electronic-specific rules?* What electronic-specific rules apply, and what requirements must be satisfied to ensure that the transaction is legally valid and enforceable? The focus here is on electronic procedural requirements applicable to all transactions, not on the substantive legal requirements for this particular transaction.
- *Security—Is the transaction trustworthy?* What is required before the parties will be comfortable relying on the transaction? How can the parties be sure who sent an electronic message or who signed an electronic record? How can the parties be sure that the record has not been altered since it was created? Are the electronic records sufficiently trustworthy such that it will be enforced by a court?

For purposes of analyzing these issues and the corresponding legal requirements for electronic transactions, it is important to differentiate between the substantive law applicable to the particular transaction under consideration and the electronic legal issues raised by that transaction. While the distinction is not always a perfect one, it is a helpful way to look at the issues.

All transactions must comply with the substantive legal requirements applicable to the specific form of transaction. Contracts involving the sale of goods, for example, must comply with substantive rules that require offer, acceptance, signature, consideration, and so forth. They are also governed by substantive rules addressing issues such as warranties, mistake, risk of loss, breach, liability, and termination.

Electronic transactions, however, must also comply with a second set of rules—i.e., a series of electronic-specific legal requirements that focus on how to do the transaction in electronic form (assuming that all of the substantive legal requirements have otherwise been satisfied). The electronic-specific legal requirements are often set forth in general purpose e-transaction laws² and address issues such as how to electronically satisfy paper-based requirements for a signature or an original and how to properly protect the interests of the various parties to the transaction.

This article assumes that the requirements of the substantive law (e.g., offer, acceptance, and consideration for contracts) are satisfied and focuses only on identifying the electronic legal issues that must be satisfied to

do any transaction in electronic form. Because such requirements can be extensive and will vary greatly depending on the nature of the transaction and the jurisdiction involved, this article will focus primarily on the basic electronic-specific issues, and it will do so without addressing detailed differences in approach that sometimes arise between various jurisdictions.

1. AUTHORIZATION—CAN THIS TRANSACTION BE DONE IN ELECTRONIC FORM?

Any effort to implement an electronic transaction project must begin with the fundamental question, “can this transaction be done in electronic form?” Answering that question begins with a clear identification of: (i) the nature of the transaction, and (ii) the various functional elements included in the transaction.

The nature of the transaction focuses on what it is—e.g., contract, promissory note, warehouse receipt, security interest, issuance of insurance policy, funds transfer payment instruction, deed, background check authorization, etc. Also, is it a consumer, business, or government transaction? The electronic rules (as opposed to the substantive rules) applicable to the transaction will often vary depending on the type of transaction involved.

The various functional elements that will be part of the transaction include, for example, requirements for signature, witnesses, notarization, delivery of documents, payment, notices, periodic statements or reports, filing with government agencies, recordkeeping requirements, and the like. Identifying these functional elements is critical, as in many cases they raise special electronic requirements that must be addressed.

Once the nature of the transaction and its functional elements have been identified, a business can proceed to address the threshold question of whether such transaction will be legally valid and enforceable in all of the relevant jurisdictions if done in electronic form.³ In most cases this involves determining whether there is an applicable general e-transaction law that authorizes the transaction (and its various elements) to be done in electronic form (or more appropriately, whether there is a law that eliminates any legal barriers to doing the transaction electronically). Often this is the easy question to address, as the answer is usually “yes,” but not in all cases.

1.1 The Primary E-Transaction Laws

The validity and enforceability of electronic transactions has been the subject of extensive worldwide legislative efforts. The U.S. federal government, all 50 U.S. states, the European Union, and the governments of most countries have enacted some form of legislation governing the en-

forceability and conduct of electronic transactions.⁴ In 2005, the United Nations approved an international treaty governing cross-border electronic contracts. Generally, such laws (referred to herein as “e-transaction laws”) support doing most transactions in electronic form if certain requirements are satisfied.

- *United States.* In the U.S., the enforceability of electronic transactions is primarily governed by: (i) the Uniform Electronic Transactions Act (UETA),⁵ 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 46 states,⁶ and (ii) the Electronic Signatures in Global and National Commerce Act (E-SIGN),⁷ a federal law enacted in 2000 that largely preempts inconsistent state law but that also defers to UETA where it has been enacted.⁸
- *European Union.* In the European Union, the enforceability of electronic transactions is governed by the Electronic Signatures Directive adopted in 1999,⁹ the Electronic Commerce Directive adopted in 2000,¹⁰ and individual country implementations of these Directives.¹¹
- *International Model Laws.* Internationally, model laws governing the enforceability of electronic transactions have also been developed by the United Nations Commission on International Trade Law (UNCITRAL),¹² which completed work on its Model Law on Electronic Commerce¹³ in 1996, and finalized and approved its Model Law on Electronic Signatures in 2001.¹⁴ These model laws have served as the basis for legislation enacted in several countries, including E-SIGN and UETA in the U.S.¹⁵
- *International Treaty.* In 2005 the United Nations approved the United Nations Convention on the Use of Electronic Communications in International Contracts (UN E-Contracting Convention).¹⁶ This international treaty was developed by UNCITRAL during the period from 2002-2005, was approved by the UN General Assembly on November 23, 2005, and is now open for ratification by all countries. It is intended to remove obstacles and enhance legal certainty and commercial predictability where electronic communications are used in connection with the formation or performance of international contracts.

U.S. and international e-transaction laws authorizing the use of electronic records and electronic signatures generally applies to most business, commercial (including consumer),¹⁷ and governmental trans-

actions. However, there are a variety of exceptions to the scope of transactions they authorize in electronic form.

In some cases there are certain types of transactions that are subject to special rules. These include electronic negotiable instruments (which raise special concerns regarding the need for a unique original)¹⁸ and electronic notarization (which raises special concerns regarding the need for physical presence, authentication, and integrity).¹⁹

In other cases, certain types of transactions are expressly excluded from the authorization provided in the statute. For example, in the U.S., E-SIGN and/or UETA expressly exclude transactions governed by all articles of the UCC (other than sections 1-107 and 1-206 and Articles 2 and 2A),²⁰ wills, codicils, or testamentary trusts, family law matters such as adoption or divorce, court orders or notices, cancellation of utility services, repossession, foreclosure, or eviction notices, cancellation of health or life insurance benefits, product recall notices, and the like.²¹ Similarly, the UN E-Contracting Convention excludes a variety of transactions. This includes consumer transactions; transactions on a regulated exchange; foreign exchange transactions; transactions involving interbank payments, or clearance and settlement systems relating to securities or other financial assets or instruments; certain securities-related transactions, and bills of exchange, promissory notes, consignment notes, bills of lading, warehouse receipts or any transferable document or instrument that entitles the bearer or beneficiary to claim the delivery of goods or the payment of a sum of money.²²

It is worth noting, however, that e-transaction laws typically do not prohibit conducting any of the excluded transactions in electronic form. Rather, the enforceability of those types of transactions is left to other law. Thus, in the case of excluded transactions, it will be necessary to look to other law to determine whether such transactions are authorized (or prohibited) in electronic form.

For most transactions, however, the question is not “whether” they can be done in electronic form, but rather “how.” Before addressing the details of the electronic-specific rules, it is important to understand the way that the e-transaction laws work.

1.2 The Basic Approach—Nondiscrimination and Functional Equivalence

E-transaction laws authorize most transactions to be conducted in electronic form. They typically do this by: (1) setting out a general principle of “nondiscrimination,” and (2) removing barriers to electronic transactions found in traditional substantive laws by adopting an approach based on the concept of “functional equivalence.”

The principle of nondiscrimination is key to most e-transaction laws. It is typically expressed as a simple statement to the effect that electronic records and electronic signatures cannot be denied legal effect or enforceability solely on the ground that they are in electronic form,²³ but it constitutes a fundamental premise: namely, that the medium in which a record, signature, or contract is created, presented, or retained does not affect its legal significance. In other words, the fact that a transaction is set forth in an electronic record, as opposed to paper, is irrelevant.²⁴

This principle should not, however, be misinterpreted as establishing the absolute legal validity of any given electronic record or electronic signature, or of any information contained in an electronic record. It merely means that the medium in which the information comprising the transaction is presented or retained cannot be used as the only reason for which that information would be denied legal effectiveness, validity or enforceability—i.e., it prohibits a court from holding that covered transactions are unenforceable solely because of the fact that they are conducted in electronic form.²⁵

The principle of nondiscrimination does not resolve concerns that an electronic transaction may still be unenforceable because it fails to satisfy the many paper-based “form” requirements frequently found in the substantive law applicable to commercial transactions. Those include requirements that the documents evidencing a transaction be: (a) “in writing,” (b) “signed,” (c) formatted or delivered in a certain manner, (d) stored or retained in a certain manner, and (e) presented or retained in “original” form.

Such form requirements have traditionally been viewed as a significant obstacle to the development of e-commerce.²⁶ In some cases they may well create a clear barrier to conducting transactions in electronic form (e.g., the risk that a statutory requirement for a signature might be interpreted to require a handwritten signature in ink on paper may be unacceptable); in other cases they raise, at the very least, uncertainty over whether electronic transactions will be enforceable. In addition, even where form requirements as such do not exist, obstacles to the use of electronic records may derive from rules of evidence that expressly or implicitly limit the parties’ ability to use electronic records as evidence to demonstrate the existence and content of contracts.²⁷

To address potential problems created by these paper-based form requirements, e-transaction laws typically adopt an approach based on the concept of “functional equivalence.”²⁸ This approach requires that paper-based commerce and electronic commerce should be treated equally by the law with respect to these form issues, so long as the electronic version of the transaction satisfies the requirements for equivalence specified in

the e-transaction law.²⁹ Those requirements are intended to replicate in the electronic world the objectives achieved by each form requirement in the paper world.

Thus e-transaction laws set forth the requirements that must be satisfied by an electronic record to establish functional equivalence to the various paper-based form requirements. This “approach is based on an analysis of the purposes and functions of the traditional paper-based requirement, with a view to determining how those purposes or functions could be fulfilled through electronic-commerce techniques.”³⁰ It “does not attempt to define a computer-based equivalent to any particular kind of paper document.” Instead, it singles out the basic functions of the primary paper-based form requirements (e.g., writing, signature, original, delivery, and record keeping), and sets out criteria that, if satisfied, enable electronic communications to enjoy the same level of legal recognition as corresponding paper documents.³¹

Through this approach, e-transaction laws seek to provide an answer to basic questions such as:

- If a law requires a “writing,” how can an electronic transaction satisfy that requirement?
- If a law requires a “signature,” how can an electronic transaction satisfy that requirement?
- If a law requires an “original,” how can an electronic transaction satisfy that requirement?
- If a law requires “delivery” in a certain manner, or by a certain time, how can an electronic transaction satisfy that requirement?
- If a law imposes a record keeping requirement, how can an electronic record satisfy that requirement?

A key advantage of the functional equivalence approach is that it allows jurisdictions to enforce electronic transactions in accordance with existing laws “without necessitating the wholesale removal of the paper-based requirements themselves or disturbing the legal concepts and approaches underlying those requirements.”³² As noted in the Prefatory Note to UETA, “By establishing the equivalence of an electronic record... [UETA] removes these barriers without affecting the underlying legal rules and requirements.”³³

At the same time, however, this approach requires establishing a series of the electronic-specific requirements that must be satisfied to create valid and enforceable electronic transactions. The key electronic requirements are discussed below.

2. ELECTRONIC REQUIREMENTS—WHAT ARE THE ELECTRONIC-SPECIFIC RULES?

Generally, there are two potential sources of “electronic” requirements for any type of transaction: (1) e-transaction laws (which apply to most transactions regardless of the applicable substantive law), and (2) the applicable substantive law governing the transaction, which will, in some cases, contain specific “electronic” requirements.

The fundamental electronic rules applicable to most (but not all) electronic transactions are found in the e-transaction laws. These laws typically apply regardless of the substantive law governing the transaction and typically focus only on the issues raised by the use of the electronic medium. Some of the requirements they impose are designed to ensure functional equivalence with the form requirements of substantive laws. Other requirements, however, seek to add protections for parties to the transaction that are deemed necessary by the use of the electronic medium (e.g., accessibility to electronic records) or that are deemed necessary to protect certain groups (e.g., consumers). Additional rules have also been adopted in some cases to answer certain “what if” questions unique to the world of electronic transactions (e.g., where is an electronic message deemed to be sent “from”?, or what if an error is introduced by the communication medium?).

In addition, the substantive laws and regulations applicable to the transaction often impose additional electronic requirements, or alternatively, impose form requirements that trigger issues under the e-transaction laws. Sometimes all of the electronic legal issues applicable to a given type of transaction are addressed in the substantive law, whereas in other cases they merely supplement the electronic legal rules found in the e-transaction laws.

Details regarding some of the more common electronic requirements that are found in both of these categories of laws are as follows.

2.1 Agreement to Engage in Electronic Transactions

Many e-transaction laws contain an express or implied requirement that the parties involved must agree to doing the transaction in electronic form. Both E-SIGN and UETA, for example, include provisions to the effect that they do not require any person to agree to use or accept electronic records or electronic signatures.³⁴

UETA also includes an express requirement that the parties agree to conduct the transaction by electronic means: “This [Act] applies only to transactions between parties each of which has agreed to conduct transactions by electronic means.”³⁵ In other words, if the parties have not agreed to conduct their transaction electronically, UETA will not apply.³⁶

Under both E-SIGN and UETA the requirement for agreement is a very general one and may often be implied from the context and surrounding circumstances of the transaction, including the conduct of the parties in taking the necessary steps to engage in an electronic transaction.³⁷ In fact UETA expressly states that: “Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties’ conduct.”³⁸ Thus there is generally a great deal of flexibility as to how such an agreement is evidenced; it typically need not be set forth in a formal express agreement and is usually not subject to specific notice requirements. However, some state variations of UETA impose limitations—e.g., Ohio provides that a consumer’s agreement to do a transaction electronically cannot be inferred solely from use of electronic means.³⁹

For most transactions, the requirement that the parties agree to do the transaction in electronic form suggests that the transaction process should be set up to evidence the requisite intent and consent. Express contract language may also be helpful. However, it should be noted that some statutes impose rules regarding the consent process. This is particularly true in the context of transactions where a party seeks to include a consent to transact business electronically in a paper contract where it might not normally be expected.

The California enactment of UETA, for example, makes clear that consent to engage in electronic transactions cannot be obtained by use of a paper-based form contract:

Except for a separate and optional agreement the primary purpose of which is to authorize a transaction to be conducted by electronic means, an agreement to conduct a transaction by electronic means may not be contained in a standard form contract that is not an electronic record. An agreement in such a standard form contract may not be conditioned upon an agreement to conduct transactions by electronic means. An agreement to conduct a transaction by electronic means may not be inferred solely from the fact that a party has used electronic means to pay an account or register a purchase or warranty. This subdivision may not be varied by agreement.⁴⁰

Other states also impose specific limitations on the manner of such consent. Louisiana appears to impose an absolute requirement for electronic consent,⁴¹ and five other states essentially prohibit the use of nonelectronic means of consent unless certain requirements are satisfied.⁴²

In addition, the right to refuse to accept electronic records may be a consideration in determining whether some transactions are feasible, par-

ticularly transactions such as electronic filings or recordings where the intended recipient might not have the capability to accept electronic records.

2.2 Consumer Consent to Receive Certain Information in Electronic Form

Separate and apart from the requirement that the parties agree to do their transaction in electronic form, E-SIGN imposes a very specific and detailed notice and consent requirement before electronic delivery of certain transaction information will be authorized. However, its application is limited. It applies: (i) only in the case of a consumer transaction, and (ii) only if “a statute, regulation, or other rule of law requires that information relating to a transaction... be provided or made available to a consumer in writing.”⁴³ This requirement also appears in some federal regulations⁴⁴ and in at least eight state enactments of UETA.⁴⁵

Under this consumer notice and consent provision, sending information in electronic form that applicable law requires be delivered “in writing” to a consumer is acceptable only if: (i) the consumer affirmatively consents to receive an electronic record in lieu of a paper, (ii) provides such consent electronically, and (iii) does so in a manner that reasonably demonstrates that he or she can access the electronic information in the form that will be used.⁴⁶ 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/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.⁴⁷

Consider, for example, the case of a consumer who sets up an online financial account and enters into an account agreement via the Internet. If the law applicable to the transaction requires the financial institution to deliver monthly statements of account to the customer in writing, and if the financial institution desires to deliver those monthly statements to its customer in electronic form, then it must first make the information disclosures required by E-SIGN and obtain the consumer's consent to receive those monthly statement electronically, before it can do so. Otherwise the financial institution will be required to continue to send the monthly statements to the consumer on paper.

Failure to make the foregoing disclosures, or failure to obtain the requisite consumer consent, does not invalidate the transaction.⁴⁸ However, the vendor must then provide the requisite information in paper form or risk being in noncompliance with the applicable substantive rule of law that requires delivery of the information to the consumer in writing.

Finally, it is important to note that UETA also includes a general requirement for agreement to electronic document delivery that applies to all parties, not just consumers. Specifically, UETA provides that where "a law requires a person to provide, send, or deliver information in writing to another person," that delivery requirement can be satisfied through the use of an electronic record "[i]f parties have agreed to conduct a transaction by electronic means."⁴⁹ Other substantive laws may also impose requirements for consent to electronic delivery. For example, several state insurance laws and regulations expressly include some type of a consent requirement before electronic delivery of transaction information is authorized.⁵⁰

2.3 Transaction Information Disclosure Requirements

Because of the nature of electronic transactions, there is sometimes a concern that a party will not completely understand who he is dealing with, what he is agreeing to, or what is happening. Thus, in some cases, applicable e-transaction law requires the delivery of certain information from vendor to customer. This is frequently (although not always) done as a consumer protection measure. These laws typically apply to online sales transactions and usually require that the vendor provide certain information to the prospective customer before the transaction is finalized.

California law, for example, requires vendors conducting business through the Internet to disclose their legal name, street address, and return and refund policy.⁵¹ Such a disclosure can be in writing or by electronic means, but it must occur before the vendor accepts any payment or processes any credit card or funds transfer. If the disclosure is made by on-screen notice, the vendor must legibly display the information ei-

ther: (i) on the first screen displayed when the vendor's electronic site is accessed, (ii) on the screen on which goods or services are first offered, (iii) on the screen on which a buyer may place the order for goods or services, (iv) on the screen on which the buyer may enter payment information, such as a credit card account number, or (v) for nonbrowser-based technologies, in a manner that gives to the user a reasonable opportunity to review that information.⁵²

The European Union Electronic Commerce Directive imposes a similar requirement. It requires that sellers of goods online provide a variety of information to the customer regarding the proposed 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 seller and where it will be accessible, the technical means for identifying and correcting input errors prior to the placing of the order, and the languages offered for the conclusion of the contract.⁵³ The seller 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.⁵⁴

2.4 Transaction 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., both E-SIGN and UETA essentially provide 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."⁵⁵

The European Union Electronic Commerce Directive contains a similar requirement. Under the Directive, "contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them."⁵⁶

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.

2.5 Signature Requirements

Not all transactions require a signature, but in many cases a transaction is governed by a law or regulation that requires the presence of a signature before it will be considered legally effective. The statute of frauds (which requires contracts for the sale of goods in excess of \$5,000 to be “signed”)⁵⁷ 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. Even in cases where a signature is not required by law, a signature may be desirable to enhance enforceability or to provide one party with additional assurance that the other party has agreed to the terms. In all such cases, the use of a legally valid and enforceable electronic signature is critical.

To be functionally equivalent to a handwritten signature and enforceable under U.S. law, both E-SIGN and UETA require that an electronic signature possess three elements:⁵⁸

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

Electronic signatures that meet these requirements are considered legally enforceable as substitutes for handwritten signatures for most transactions in the U.S.⁵⁹

Symbol. The U.S. 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;⁶⁰
- A digitized image of a handwritten signature that is attached to an electronic document;
- 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);⁶¹
- 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).⁶²

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.

Attached. Another important aspect of this definition lies in the necessity that the electronic signature be linked to or logically associated with the record being signed. In the paper world, it is assumed that the symbol adopted by a party as his signature is attached to or located somewhere in the same paper that the signer intends to sign. However, since electronic records can be communicated separate from any tangible media on which they may exist, this definition requires that the signature must, in some way, be “attached to or logically associated with” the electronic record being signed.⁶³

This 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.

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.

Existence of appropriate intent is critical to qualifying as a signature. For example, one court held that the sender's phone number (i.e., a symbol) appended to a faxed document could qualify as a signature. However, the court concluded that, under the facts of that case, it was not a signature since it was automatically applied by the fax machine that sent the fax, and was not appended by the sender with intent to sign the particular fax in issue.⁶⁴

Thus it is important that the process by which an electronic signature is applied to a document be set up in a manner designed to ensure that the application of the signature is done in a way to evidence the intent of the signer to sign or otherwise be bound by the document. This is usually accomplished by the context in which the signature is applied, just as the language at the end of a paper contract and immediately preceding the handwritten signature usually indicates the intent associated with the signature.

In other countries (as well as under the UN E-Contracting Convention) the requirements for a valid electronic signature can be somewhat different.

2.6 Method of Electronic Delivery

UETA and E-SIGN do not specify the method by which electronic document delivery may be accomplished. UETA, however, defers to substantive law governing the transaction.

If the substantive law requires delivery of a document and specifies a particular method of delivery (e.g., registered mail), then UETA requires that such delivery method be used.⁶⁵ In other words, UETA authorizes the use of electronic documents, but it does not affect any requirement imposed under the substantive law governing the format or delivery of any documents, other than a requirement that the documents be in paper form.⁶⁶ Thus UETA provides that where another law requires a document to be "sent, communicated, or transmitted by a specific method" (e.g., registered mail), then the electronic record must be sent, communicated, or transmitted by the method specified in that other law.⁶⁷

This is a savings provision for laws that provide for the means of delivering information, and thus such laws are not affected by UETA. For example, if a law requires delivery of notice by first class U.S. mail, that requirement would not be affected by UETA. The information to be delivered may be provided on a disk (i.e., in electronic form), but the particular means of delivery must still be via the U.S. Postal Service. Such delivery requirements in existing law will continue to be applicable to electronic records.⁶⁸

It is also important to note that those delivery requirements, as specified in the applicable substantive law, cannot be varied by agreement, except to the extent permitted by such other law.⁶⁹

Where electronic delivery is appropriate, effective electronic delivery is generally construed to require that the recipient have the ability to download, print, and otherwise retain a copy of the document in his own possession, just as he would have in the case of paper. As the UETA comments point out, “to meet a requirement of other law that information be provided in writing, the recipient of an electronic record of the information must be able to get to the electronic record and read it, and must have the ability to get back to the information in some way at a later date.”⁷⁰ Thus the mere ability to view a document on a computer screen is not usually considered to be delivery.

Both UETA and E-SIGN recognize that recipients have different levels of computing capabilities, and some may not have the capabilities necessary to download, print, or otherwise retain a copy of the document. Thus they generally put the burden on the sender to use a form of communication such that the information is capable of being downloaded, printed, and saved, but do not make the sender responsible for the actual computer capabilities of the recipient.⁷¹

Accordingly, UETA provides that an electronic record is not enforceable against the recipient if the sender inhibits the ability of a recipient to store or print an electronic record.⁷² Likewise, E-SIGN 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.”⁷³ Other regulations take a similar approach.⁷⁴

Finally, a key question for any electronic delivery is whether the intended recipient actually received the document. When delivery is made via the U.S. Postal Service, there is a legal presumption of receipt that arises when a properly addressed letter is mailed. No such presumption arises from electronic delivery as of yet.

Noting that providing information through postal mail provides reasonable assurance that the delivery requirement is satisfied, the SEC takes the position that persons providing electronic delivery of information should similarly have reason to believe that any electronic means so selected will result in the satisfaction of the delivery requirements. According to the SEC, examples of procedures evidencing satisfaction of the delivery requirements include: (1) obtaining an informed consent from a person to receive the information through a particular electronic medium coupled with assuring appropriate notice and access; (2) obtaining evidence that an intended recipient actually received the information, for example, by electronic mail return-receipt or confirmation of accessing, downloading, or printing; (3) disseminating information

through certain facsimile methods; (4) establishing that an intended recipient accessed a document with hyperlinking to the document to be delivered; and (5) using forms or other material available only by accessing the information.⁷⁵

The Department of Labor, on the other hand, takes the position that delivery requirements are satisfied if the sender takes appropriate and necessary measures reasonably calculated to ensure that the system for furnishing documents results in actual receipt of transmitted information (e.g., using return-receipt or notice of undelivered electronic mail features, conducting periodic reviews or surveys to confirm receipt of the transmitted information).⁷⁶

2.7 Electronic Record Format Requirements

As a general matter, neither E-SIGN nor UETA impose any format requirements. The underlying substantive law governing the transaction may, however, specify the “format” a document must use. In such a case, neither E-SIGN nor UETA affect any such requirement (other than a requirement that documents be in paper form).⁷⁷ Thus UETA provides that where another law requires a record to “contain information that is formatted in a certain manner” then the electronic record must contain the information formatted in the manner specified in that other law,⁷⁸ and where another law requires a record to be posted or displayed in a certain manner, then the electronic record must be posted or displayed in the manner specified in that other law.⁷⁹

This is a savings provision for laws that provide for the means of displaying information, and thus such laws are not affected by UETA. Such display and formatting requirements in existing law will continue to be applicable to electronic records. If those legal requirements can be satisfied in an electronic medium, e.g., the information can be presented in the equivalent of 20-point bold type as required by other law, UETA will validate the use of the medium, leaving to the other applicable law the question of whether the particular electronic record meets the other legal requirements.⁸⁰

2.8 Electronic 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 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;⁸¹ and
- remains accessible for later reference.⁸²

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.⁸³ This provision also makes 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.

This rule requires that there exist reliable assurance that the electronic record accurately reproduces the information. This is consistent with Fed. R. Evid. 1001(3) and Unif. R. Evid. 1001(3) (1974). This rule assures that information stored electronically will remain effective for all audit, evidentiary, archival and similar purposes. The requirement of accuracy is derived from the Uniform and Federal Rules of Evidence. The requirement of continuing accessibility addresses the issue of technology obsolescence and the need to update and migrate information to developing systems.

3. SECURITY—IS THE TRANSACTION TRUSTWORTHY?

The third key concern for businesses seeking to engage in electronic transactions is the 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. Clicking on an “I Agree” button, for example, can create a legally valid electronic signature, but if it becomes necessary to enforce that transaction in court, how do you prove “who” clicked?

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 trans-

action. Trust means many things in many situations.⁸⁴ Trusting one's business partners has always been important (e.g., are they reputable and creditworthy? will they perform as promised?). In today's e-business environment, however, companies also need to trust the transaction itself.

Ensuring that we can trust the transaction requires addressing a variety of issues. Are the electronic records accurate, such that each party (and third parties) can rely on them? Can the identity of the creator/sender/signer of each electronic record be reliably verified if necessary? Will each electronic record be admissible in court? Are they properly protected, so as to prevent any compromise that might result in injury to the business or others? Are they accessible and available as needed, and adequately protected from media deterioration and technical obsolescence? While these issues arise to some extent in paper-based transactions, they are in many respects uniquely electronic issues. "Trust is central to e-commerce."⁸⁵

Information security is the method used to help establish a level of "trust" in electronic information appropriate to the situation. That is, through the implementation of appropriate information security measures, businesses seek to ensure a reasonable level of trust in the accuracy of the identity of the person who created, signed, and/or sent an electronic record, trust that the record has not been altered without authorization, and trust that contents of the record have been and will be kept confidential. As the OECD has recently noted: "By practicing sound security principles, organizations will contribute towards building trust in the use of technologies that facilitate online transactions."⁸⁶

3.1 Security Basics

Ensuring that an electronic transaction is trustworthy, from a legal perspective, requires consideration of authenticity, availability, and integrity.

(A) AUTHENTICATION

Authentication of identity⁸⁷ is critical to establishing trust in an electronic environment.⁸⁸ Quite simply, it provides a level of assurance as to whether someone or something is who or what it claims to be in a digital environment.⁸⁹

In any electronic transaction, the recipient must be reasonably certain that the person submitting and/or signing an electronic communication is the person identified in the communication.⁹⁰ This requires authenticating the identity of the sender/signer—i.e., determining whether someone is, in fact, who they are declared to be. As such, it involves confirming the asserted identity of a person, in order to determine, for example, who

is the source or origin of a communication.⁹¹ Who created or signed the document? Who sent the message? Is it genuine or a forgery?

Likewise, any use of or reliance on electronic records often requires evidence to verify that the person who purportedly created/sent/signed such record did in fact do so. And where someone wants to access stored electronic records (such as sensitive personal information), verifying their identity (as part of the process of determining whether they are authorized to have such access) is critical to protecting those records.

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.⁹² Likewise, when that same bank receives an online inquiry from someone seeking to access, edit, or copy their account information, it must verify the identity of such person, and his/her authorization to access the requested personal information.⁹³ Also, of course, if a subsequent dispute arises, the bank must be able to satisfy a court (with admissible evidence) as to the identity of the person who requested the funds transfer or the identity of the person to whom it granted access to the account information.⁹⁴

(B) AVAILABILITY OF DATA

Data kept in electronic form is not readily viewable or readable by a human being. To make use of the data, it must be on a storage device that can be accessed by an appropriate computer or other machine, and that machine must include software capable of reading and interpreting the digital data in order to display it in a human readable form. Moreover, the medium on which the data resides must be physically intact and undamaged so that the foregoing processes can take place. And of course, threats resulting from media deterioration or software or hardware obsolescence must be addressed.

Generally, the security concept of availability involves ensuring that the computer systems, networks, and data are operational, fully functioning, available for use, and accessible whenever needed. One statute, for example, defines “availability” simply as “ensuring timely and reliable access to and use of information.”⁹⁵ In other words, availability is often used simply to refer the ability to access and read information when needed.

(C) DATA INTEGRITY

Data integrity is concerned with the accuracy and completeness of information, such as electronic records and messages communicated over the Internet or stored on a party’s system, and with ensuring that

no unauthorized alterations are made to such data either intentionally or accidentally. Ensuring “integrity” requires “guarding against improper information modification or destruction, [including] ensuring information nonrepudiation and authenticity.”⁹⁶ Relevant questions include: 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 records 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.

In an electronic transaction of any significance, the recipient of an electronic message must be confident of the identity of the sender and the integrity of the communication before the recipient relies and acts on the message. Both are critical to e-commerce. Some courts have started requiring expanded proof of the integrity of stored electronic records before they will be admissible as evidence in the case.⁹⁷

3.2 Security and the Enforceability of Electronic Transactions

Most major e-transaction laws, such as E-SIGN, UETA, the EU Electronic Signatures Directive, and the UN E-Contracting Convention require the use of security for a variety of purposes.

In almost all cases, e-transaction laws use some elements of information security as the means by which the parties establish functional equivalence to paper-based form requirements for a “writing” and “signature” (such as those found in the statute of frauds), and requirements for an “original” (such as those found in the rules of evidence). Specifically, without ever using the word “security” these electronic transaction statutes require the use of information security as follows:

- To satisfy “writing” requirements, measures to ensure the availability of the data must be implemented. For example, to satisfy requirements that a document be in “writing,” E-SIGN requires that an electronic record be “capable of being retained and accurately reproduced for later reference by,”⁹⁸ UETA requires that the electronic record be “retrievable in perceivable form,”⁹⁹ and the UN E-Contracting Convention requires that the information in an electronic communication must be “accessible” and “usable for subsequent reference.”¹⁰⁰

- To satisfy “signature” requirements, measures to authenticate the identity of the signer and to ensure the integrity of evidence of intent are required. In the U.S., both E-SIGN and UETA require use of a sound, symbol, or process that is attached to or associated with the record being signed and executed or adopted by a person with the intent to sign the record.¹⁰¹ The EU Electronic Signatures Directive requires “data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.”¹⁰² The UN E-Contracting Convention requires establishing the identity and the intent of the party signing an electronic communication in a manner that is as reliable as appropriate under the circumstances.¹⁰³
- To satisfy requirements that the “original” of a document be provided, made available, or retained, measures to ensure the integrity and the availability of the data must be implemented. In the U.S., both E-SIGN and UETA require that the electronic record must “accurately reflect the information” and must “remain accessible” to all persons who are entitled to access.¹⁰⁴ The UN E-Contracting Convention requires “a reliable assurance as to the integrity of the information” contained in an electronic communication and that it must be “capable of being displayed to the person to whom it is to be made available.”¹⁰⁵

Security is also used as a risk allocation device in some e-transaction laws. This is particularly true in U.S. law such as UETA and U.C.C. Article 4A regarding electronic funds transfers. Under UETA, if a change or error in an electronic record occurs in a transmission between the parties to a transaction, the use of—or failure to use—an agreed-upon security procedure will determine who bears the risk of loss.¹⁰⁶ Likewise, in U.C.C. Article 4A, the determination as to whether the bank or its customer bears the risk of a fraudulent electronic payment instruction will turn on whether the bank used a commercially reasonable security procedure for authenticating the identity of its customer and detecting an error in the transmission or content of the electronic communication.¹⁰⁷

4. PUTTING IT ALL TOGETHER—THE CRITICAL ROLE OF “PROCESS”

Finally, when setting up the procedures for any electronic transaction it is important to carefully review the proposed “process” in order to gain a clear understanding of what will happen and how it will occur. This is critical for determining whether all of the relevant electronic-specific requirements will be satisfied, identifying any new legal issues that may

be raised, and identifying those elements of the process that may need to be changed or restructured in order to ensure legal compliance.

For example, something as simple as an online contracting process that does not allow the other party to print or download a copy of the contract may present significant enforceability problems. Similarly, if electronic signatures are not attached or linked to the electronic record being signed, they may not be valid. Likewise, an online contracting process that does not properly authenticate the identity of the other party presents both enforceability and admissibility issues in the event of a subsequent dispute.

Thus it is important for any electronic transaction to begin with a clear and comprehensive understanding of the process involved and how it will actually work from a technical perspective. In fact, understanding “how it works” from a technical perspective is critical to “making it work” from a legal perspective.

Understanding the process typically requires that the lawyer consult closely with both the business and technical personnel involved. In many cases, the company may have made assumptions about how the process will work without a rigorous comparison of the technical details of that process to the legal requirements. As a result, it frequently turns out that the process that the company has implemented—or intends to implement—is not adequate to address applicable legal concerns.

Identifying the relevant technical issues requires close coordination with the appropriate people involved in the implementation. The biggest obstacle is often getting past assumptions and generalizations made by such personnel, both business and technical, regarding how the process will work. Thus it is important to ask probing questions regarding the details of how the process will be implemented. This requires forcing them to drill down and provide highly specific details of certain aspects of the process (e.g., What will be used as the signature in this transaction?, How is it captured?, How will the electronic signature be attached or linked to the electronic record?, How and in what format will the record of the contract be stored?, and How will the signer be authenticated?). Often, the only way to get the answers to these questions is to speak directly with the persons involved in developing or implementing the electronic processes. In many cases, the technical staff is just not aware that the use of a certain procedure, or a particular choice of approach, can have a significant legal impact.

Once the proposed technical processes have been identified and explained, it is important to undertake a detailed analysis of those processes to determine whether they satisfy all of the relevant electronic-specific requirements and to identify any legal issues that they raise. When doing

so, also recognize that a given process may raise issues in one jurisdiction but not another or may raise one set of issues in one jurisdiction and a different set of issues in another jurisdiction. For example, in some countries, electronic signatures must identify the signer, whereas in other countries a simple click on an “I Agree” button is sufficient. Similarly, methods used for online authentication may be legally sufficient in some jurisdictions and not in others.

The focus is on the impact of the proposed process on the electronic-specific procedural legal requirements for the transaction. In many cases, identification of these issues will require a reexamination of some of the technical details, as well as a review of the applicable legal requirements in the affected jurisdictions.

Throughout this strategic process, accurately and adequately understanding the technical process involved is perhaps most essential to a successful outcome. Everything regarding compliance with the electronic-specific requirements of e-transaction laws and general substantive laws will hinge on the way that the electronic process operates, and it may be necessary for the lawyer to specify how it should be modified. This is also critical with respect to compliance with privacy and data security laws that may be applicable to the information involved in the transaction.

The most dangerous mistake that can be made is to make assumptions (or accept assumptions by others) about the process without verifying how exactly it will work and what exactly will happen. Making assumptions can be very dangerous. For example, one might assume that because data is “encrypted,” it is adequately protected. It is critical, however, to look behind that general statement to evaluate what is encrypted, how it is encrypted, when the encryption is applied, who has access to the encrypted data, when and how the data is used in unencrypted form, whether the encryption algorithms and key lengths are adequate, who has access to the decryption keys, and other relevant concerns. Likewise, merely assuming that the other party to a transaction is adequately authenticated because he or she is required to use a user ID and password can lead to serious problems. It is important to look behind that process to address questions such as how the user IDs and passwords are associated with and assigned to a particular person, what opportunities are available for other persons to obtain access to those user IDs and passwords, and how easily those IDs and passwords are compromised.

5. CONCLUSION

Almost all transactions can be done in electronic form. The difficult issues are determining which electronic-specific requirements must be addressed to satisfy applicable e-transaction laws, determining which

security measures are required to ensure the transaction is considered trustworthy, and then implementing an appropriate process to accomplish both.

NOTES

1. “Transaction” is defined broadly to mean “an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons.” See 15 U.S.C.A. § 7006(13).

2. They also appear in some substantive laws.

3. For purposes of this discussion, we assume that the fundamental legal elements required for any particular type of transaction are otherwise present and satisfied. For example, if the contemplated electronic transaction involves entering into a contract, this article assumes that the basic requirements of a contract under applicable law—e.g., offer, acceptance, consideration, etc.—will be present, and focuses only on the additional requirements for enforceability that arise because of the electronic nature of the transaction.

4. For a comprehensive list of all such laws, see Mason, *Electronic Signatures in Law* (2007), at Appendix 1.

5. Uniform Electronic Transactions Act (UETA), approved by the National Conference of Commissioners on Uniform State Laws (NCCUSL) on July 23, 1999. A copy of UETA is available at <http://www.law.upenn.edu/bl/ulc/fnact99/1990s/ueta99.htm>.

6. As of August, 2008, 46 states and the District of Columbia had enacted UETA. For an updated list of those states that have enacted UETA, see http://www.nccusl.org/Update/uniformact_factsheets/uniformacts-fs-ueta.asp.

7. Electronic Signatures in Global and National Commerce Act (E-SIGN), 15 U.S.C.A. § 7001 et. seq., effective October 1, 2000. E-SIGN is available at <http://www.ntia.doc.gov/ntiahome/frnotices/2002/esign/report2003/ElectronicSignaturesAct.pdf>. E-SIGN preempts all inconsistent state legislation, other than state enactments of UETA in the form promulgated by NCCUSL.

8. See E-SIGN, 15 U.S.C.A. § 7002.

9. Directive 1999/93/EC of 13 December 1999 on a Community Framework for Electronic Signatures (Electronic Signatures Directive). A copy of the Electronic Signatures Directive is available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML>.

10. 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 (Electronic Commerce Directive), available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML>.

11. See generally, “The Legal and Market Aspects of Electronic Signatures,” September 2003, at Appendix 4 for a country-by-country list of e-transaction laws in the EU, available at http://europa.eu.int/information_society/eeurope/2005/all_about_security/electronic_sig_report.pdf.

12. The United Nations Commission on International Trade Law (UNCITRAL) was established by the General Assembly in 1966 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 60 member states elected by the

General Assembly so as to be representative of the 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 <http://www.uncitral.org>.

13. See United Nations, UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996, available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html.

14. See United Nations, UNCITRAL Model Law on Electronic Signatures 2001 http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html.

15. Both E-SIGN and UETA borrow heavily from the Model Law on Electronic Commerce. UNCITRAL maintains a list of countries that have adopted the Model Law on Electronic Commerce, which is available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model_status.html, and the Model Law on Electronic Signatures, which is available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_status.html.

16. The 2005 United Nations Convention on the Use of Electronic Communications in International Contracts (UN E-Contracting Convention) is available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html. See also UN Press release at <http://www.un.org/News/Press/docs/2005/ga10424.doc.htm>.

17. The UN E-Contracting Convention, however, excludes consumer transactions from its scope. Article 2(1)(a).

18. See E-SIGN, 15 U.S.C.A. § 7008, and UETA § 16.

19. See E-SIGN, 15 U.S.C.A. § 7001(g), and UETA § 11.

20. This means, for example, that transactions governed by U.C.C. 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).

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

22. See UN E-Contracting Convention, Article 2.

23. See, e.g., E-SIGN, 15 U.S.C.A. § 7001(a) (“a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form”); UETA § 7(a) (“A record or signature may not be denied legal effect or enforceability solely because it is in electronic form”); Electronic Signature Directive, Article 5(2) (“Member States shall ensure that an electronic signature is not denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is:—in electronic form”); UN E-Contracting Convention, Article 8(1) (“A communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication”). See also UNCITRAL Model Law on Electronic Commerce, Articles 5, 6, and 7.

24. See UETA § 7, Comment 1; Explanatory Note by the UNCITRAL Secretariat on the United Nations Convention on the Use of Electronic Communications in International Contracts (UN E-Contracting Convention, Explanatory Note), at Para. 129.

25. See UETA § 7, Comment 1; UN E-Contracting Convention, Secretariat Explanatory Note, Para. 129.

26. Although this is clearly the prevailing view, and the most cited basis for enacting e-commerce statutes, there is some question, at least in common-law countries,

as to whether form requirements for a “writing,” a “signature,” and an “original” do constitute legal obstacles to e-commerce. See, e.g., Reed, *What Is a Signature?*, 3 *Journal of Information, Law and Technology* (2000), and reference to case law therein, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/reed, and Smedinghoff and Bro, *Moving With Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce*, 17 *J. Marshall J. Computer & Info. L.* 723 (Spring 1999), also available at <http://www.wildman.com/resources/articles-pdf/movingwithchange.pdf>.

27. See “Legal aspects of electronic commerce, Electronic contracting: background information,” Note by the Secretariat, 15 September 2003, A/CN.9/WG.IV/ WP.104/Add.3, Para. 2 <http://www.uncitral.org>.

28. UN E-Contracting Convention, Explanatory Note, at Para. 133.

29. This concept of functional equivalence appears in most e-transaction laws, including E-SIGN and UETA in the U.S., the EU Electronic Signatures Directive, the UNCITRAL Model Law on Electronic Commerce, the UNCITRAL Model Law on Electronic Signatures, and the UN E-Contracting Convention.

30. UN E-Contracting Convention, Explanatory Note, Para. 51. See, e.g., UETA § 16 (and associated Comments), which uses the concept of “control” to establish functional equivalence with the paper-based requirement for a unique original in the case of negotiable promissory notes under UCC Article 3 and documents of title under UCC Article 7.

31. UN E-Contracting Convention, Explanatory Note, Para. 51.

32. See UN E-Contracting Convention, Explanatory Note, Para. 52.

33. UETA, Prefatory Note, p.1.

34. UETA § 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”); E-SIGN, 15 U.S.C.A. § 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”). See also UN E-Contracting Convention, Article 8(2) (“Nothing in this Convention requires a party to use or accept electronic communications, but a party’s agreement to do so may be inferred from the party’s conduct”).

35. UETA § 5(b).

36. In such case, there may be significant legal uncertainty as to whether the electronic transaction is legally viable.

37. UETA § 5(b), and Comments 3 and 4.

38. UETA § 5(b).

39. Ohio Rev. Code § 1306.16(B).

40. Cal. Civ. Code, § 1633.5(b).

41. La. Rev. Stat. 22:212(7)(c).

42. Arizona (Rev. Stat. § 44-7051(C)), California (Civil Code § 1633.5(b)), North Carolina (§ 66-327(d)), Ohio (Rev. Code § 1306.16(A)), and Pennsylvania (73 P.S. § 2260.901)

43. E-SIGN, 15 U.S.C.A. § 7001(c).

44. See, e.g., Department of Labor regulations at 29 C.F.R. § 2520.104b-1(c)(2)

45. Alabama Code § 8-1A-8(e) (imposes E-SIGN consent requirement where law requires “in writing” delivery of information to consumers); Arizona Rev. Stat. § 44-7051 (specifies rules for non-electronic notices, but applicable only “If a consumer law, other than this chapter, requires a paper record or notice of the transaction”); New Jersey Stat. Ann. § 12A:12-21 (imposes E-SIGN consent requirement where law requires “in

writing” delivery of information to consumers); North Carolina Gen. Stat. § 66-327 (imposes E-SIGN consent requirement where law requires “in writing” delivery of information to consumers; but also imposes special rule where consumer uses equipment of seller); Tennessee Code Ann. § 47-10-122 (expressly states that it does not supersede E-SIGN consent requirement where law requires “in writing” delivery of information to consumers); Texas Ins. Commissioner’s Bulletin B-0002-02 (expressly states that Texas UETA—S.B. 393 §6(a)—does not modify the E-SIGN consent requirement where law requires “in writing” delivery of information to consumers); Vermont Stat. Ann. tit. 9, § 287 (imposes E-SIGN consent requirement where law requires “in writing” delivery of information to consumers); West Virginia Code § 39-A-2-1 (imposes E-SIGN consent requirement where law requires “in writing” delivery of information to consumers).

46. E-SIGN, 15 U.S.C.A. §§ 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.

47. E-SIGN, 15 U.S.C.A. § 7001(c)(1)(B).

48. E-SIGN, 15 U.S.C.A. § 7001(c)(3).

49. UETA § 8(a). Although § 8(a) appears to apply only when a law requires that the information be delivered “in writing,” the general consent rule of § 5(b) would likely apply even where no such “in writing” requirement applied.

50. Alaska, Div. of Ins. Bulletin B 04-15 (“if a consumer agrees to electronic delivery of information”); Arkansas, Ins. Dept. Bulletin No. 6-2002 (where agreed to by the parties involved); California, Cal. Ins. Code § 2689.10 (if the consumer agrees); Kentucky, §304.14-230(1) (if agreed to by both parties); Louisiana, La. Rev. Stat. Ann. § 22:212(7)(c) (insurer and policyholder or insured shall agree electronically to electronic delivery); Nevada, Bulletin No. 03-001, Jan 29, 2003 (Ref to §719.220 of NETA “whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances...”); New York, Bulletin of July 6, 2004 (if consented to by the policyholder); Ohio, Ins. Dept. Bulletin No. 2001-3 (“where agreed to by the parties involved”); Pennsylvania, §2260.901 (must contain provision specifically agreed to by consumer); South Carolina, Bulletin 2003-05 April 24, 2003 (Consent must demonstrate electronic access); Texas, Bulletin B-0012-00, Feb. 16, 2000; Bulletin B-0002-02 Jan 16, 2002 re UETA; West Virginia, WV Informational Letter No. 135, July 2002 (“If the parties have agreed to transact business electronically”).

51. Cal. Bus. & Prof. Code § 17538(d).

52. Cal. Bus. & Prof. Code § 17538(d)(2)(A).

53. EU Electronic Commerce Directive, Article 10(1).

54. EU Electronic Commerce Directive, Article 11(1) and 11(2). The UN E-Contracting Convention does not impose any information requirement like that in the EU Electronic Commerce Directive. However, it also makes clear that it does not override any rule of law that may require disclosure of such information. See UN E-Contracting Convention, Article 7.

55. E-SIGN, 15 U.S.C.A. § 7001(e). See also UETA § 8(c) (“if a sender inhibits the ability of a recipient to store or print an electronic record, the electronic record is not enforceable against the recipient”).

56. EU Electronic Commerce Directive, Article 10(3).

57. U.C.C. Article 2-201(1) (2003).
58. E-SIGN, 15 U.S.C. § 7006(5) and UETA § 2(8) (definitions of “electronic signature”).
59. See UETA §§ 2(8) and 7(d) and E-SIGN, 15 U.S.C.A. § 7001(a) and 7006(5).
60. See, e.g., *Stevens v. Publicis, S.A.*, 50 A.D.3d 253, 854 N.Y.S.2d 690, 27 I.E.R. Cas. (BNA) 1064 (1st Dep’t 2008), leave to appeal dismissed, 10 N.Y.3d 930, 2008 WL 2550684 (2008); *Polyad Company v. Indopco Inc.*, 2007 WL 2893638 (N.D. Ill. 2007); *Rosenfeld v. Zern*, 2004 N.Y. Slip Op. 24143 (2004); *Shattuck v. Klotzbach*, 14 Mass. L. Rptr. 360, 2001 WL 1839720 (Mass. Super. Ct. 2001).
61. 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 also EU Electronic Signatures Directive at Article 2(1).
62. For an overview of this technology and the process by which digital signatures are created, see Information Security Committee, Electronic Commerce Division, ABA § of Science & Technology Law, Digital Signature Guidelines, August, 1996, available at <http://www.abanet.org/scitech/ec/isc/dsgfree.html>; Smedinghoff, Ed., *Online Law*, chs. 3, 4, 31 (1996); Ford and Baum, *Secure Electronic Commerce* (1997).
63. See UETA, § 2(8), comment 7. This is consistent with the approach taken by the Food and Drug Administration in its regulations on electronic signatures set forth at 21 CFR Part 11 (March 20, 1997). Section 11.70 of those regulations also require that electronic signatures “shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.”
64. See, for example, *Parma Tile Mosaic & Marble Co., Inc. v. Estate of Short*, 87 N.Y.2d 524, 640 N.Y.S.2d 477, 663 N.E.2d 633 (1996). See also *Kohlmeyer & Co. v. Bowen*, 126 Ga. App. 700, 192 S.E.2d 400, 11 U.C.C. Rep. Serv. 565 (1972) (a securities brokerage firm’s name was printed on a confirmation statement for the sale of securities. The court found the printed name was intended as authentication, and met the signature requirement under the statute of frauds).
65. UETA § 8(b).
66. See UETA § 8(b), Comment 4.
67. UETA § 8(b)(2).
68. UETA § 8(b), Comment 4.
69. UETA § 8(d).
70. UETA § 8(a), Comment 3.
71. Except, of course, in the case of the E-SIGN consumer consent requirements, which require that the recipient’s consent to the electronic delivery of information must “reasonably demonstrate” the consumer’s ability to read the information in the form in which it will be delivered.
72. UETA §§ 8(a) and (c).

73. E-SIGN 101(e).
74. See, e.g., 1995 SEC Securities Act Release No. 7233, Exchange Act Release No. 36345 (October 6, 1995), 60 FR 53458 (October 13, 1995) (1995 SEC Release), at p. 8-9.
75. 1995 SEC Release, at pp. 10-11.
76. 29 C.F.R. § 2520.104b-1(c)(1)(i)(A).
77. See, UETA § 8(b), Comment 4; Regulation Z, 12 C.F.R. Part 226 Supplement I (Official Staff Interpretations), Comment 36(b)-1.
78. UETA § 8(b)(3).
79. UETA § 8(b)(1). See also the Department of Labor regulations at 29 C.F.R. § 2520.104b-1(c)(1)(ii) (“The electronically delivered documents [must be] prepared and furnished in a manner that is consistent with the style, format and content requirements applicable to the particular document”).
80. UETA § 8(b), Comment 4.
81. 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.A. § 7001(d)(2); UETA § 12(b).
82. UETA § 12(a); E-SIGN, 15 U.S.C.A. § 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.
83. E-SIGN, 15 U.S.C.A. § 7001(d)(3); UETA § 12(d).
84. See, e.g., McCullagh, E-Commerce—A Matter of TRUST, available at <http://www.acs.org.au/president/1998/past/io98/etrust.rtf> (arguing that “In the electronic commerce environment the concept of trust involves the interaction of four disparate components. These components are: (a) Technology Trust; (b) Behavioral Trust; (c) Product Trust; and (d) Legal Trust”).
85. OECD Policy Brief, “Electronic Commerce”, July 2001, at p. 2; <http://www.oecd.org/dataoecd/5/11/2346217.pdf>.
86. OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication, June 2007, at p. 23; available at <http://www.oecd.org/dataoecd/32/45/38921342.pdf>.
87. The term “authenticate” or “authentication” is the subject of much confusion. This is due, in part, to the fact that the term is used in two very different ways in the legal environment. U.S. courts have used the word “authenticate” in two broad senses: (1) to verify or confirm the identity or origin of (i.e., to verify that a person, document, or thing is what it purports to be), or (2) to give a legal or binding effect to (e.g., to sign). In this article, “authentication” or “to authenticate” is used in the former sense—i.e., to verify that a person is who he or she purports to be; to verify identity.
88. See, e.g., OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication, June 2007, at p. 7; available at <http://www.oecd.org/dataoecd/32/45/38921342.pdf> (noting that “electronic authentication plays a key role in the establishment of trust relationships for electronic commerce”).
89. OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication, June 2007, at p. 7; available at <http://www.oecd.org/dataoecd/32/45/38921342.pdf>.
90. See, e.g., IRS Announcement 98-27, effective April 13, 1998; 1998-15 I.R.B. 30, Paragraph (1) (setting forth rules for electronic submission of W-9 forms and requiring that “The design and operation of the electronic system, including access procedures,

must make it reasonably certain that the person accessing the system and submitting the Form W-9... is the person identified in the form”).

91. See Fed. R. Evid. 901(a) (1995). The Homeland Security Act of 2002 defines authentication as “utilizing digital credentials to assure the identity of users and validate their access.” See Homeland Security Act of 2002 § 1001(b), amending 44 U.S.C.A. § 3532(b)(1)(D).

92. See, e.g., U.C.C. Article 4A, § 202.

93. See, e.g., Federal Financial Institutions Examinations Council, “Authentication in an Internet Banking Environment,” October 12, 2005 (“FFIEC Guidance”), available at http://www.ffiec.gov/pdf/authentication_guidance.pdf. This was later supplemented by an FAQ titled “Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment,” August 8, 2006, available at http://www.ncua.gov/letters/2006/CU/06-CU-13_encl.pdf.

94. See, e.g., *U.S. v. Eisenberg*, 807 F.2d 1446, 22 Fed. R. Evid. Serv. 352 (8th Cir. 1986) (disputing the authenticity of letter); *U.S. v. Grande*, 620 F.2d 1026, 27 Cont. Cas. Fed. (CCH) P 80367, 6 Fed. R. Evid. Serv. 696 (4th Cir. 1980) (disputing authenticity of invoice).

95. See, e.g., U.S. Homeland Security Act of 2002 § 1001(b), amending 44 U.S.C.A. § 3532(b)(1)(C).

96. Homeland Security Act of 2002 § 1001(b), amending 44 U.S.C.A. § 3532(b)(1)(A).

97. See, e.g., *In re Vee Vinhnee*, 336 B.R. 437 (B.A.P. 9th Cir. 2005); *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534, 73 Fed. R. Evid. Serv. 446 (D. Md. 2007); *Victory Memorial Hosp. v. Rice*, 143 Ill. App. 3d 621, 97 Ill. Dec. 635, 493 N.E.2d 117 (2d Dist. 1986).

98. E-SIGN, 15 U.S.C.A. § 101(e).

99. UETA §§ 2(13) and 7(c).

100. UN E-Contracting Convention, Article 9(2).

101. E-SIGN, 15 U.S.C.A. § 106(5); UETA §§ 2(8) and 7(d).

102. EU Electronic Signature Directive, Article 2(1). This Directive also requires extensive security for its advanced electronic signature. See Article 2(2) and Annexes I, II, III, and IV.

103. UN E-Contracting Convention, Article 9(3).

104. E-SIGN, 15 U.S.C.A. § 101(d); UETA § 12. In the U.S., these same security requirements are also necessary to satisfy legal record retention obligations. E-SIGN, 15 U.S.C.A. § 101(d); UETA § 12.

105. UN E-Contracting Convention, Article 9(4).

106. UETA § 10.

107. U.C.C. Article 4A, §§ 201 and 202.