

Electronic Banking Law and Commerce REPORT

June 2006, Volume 11, Number 5

© Thomson/West Legalworks

THOMSON
★

E-Transactions: The Key Rules for Ensuring Enforceability

By Thomas J. Smedinghoff

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, proxy agreements, and the like. For all such transactions, companies must address a fundamental question: what are the legal requirements for conducting these transactions in electronic form?

At the same time, the rules for conducting business transactions in electronic form are rapidly coming together in most U.S. and international jurisdictions. The recently approved *United Nations Convention on the Use of Electronic Communications in International Contracts*¹ is but the latest chapter in the development of the law governing the rules for electronic transactions. This article will address the major e-transaction laws, and summarize the key legal requirements for entering into a transaction using electronic means.

Like all transactions, electronic transactions involve documents (usually referred to as “records” or “electronic records”), and signatures (usually referred to as “electronic signatures”), that are created, communicated, and stored in electronic form. They can be created through the manual efforts of an individual (e.g., typing an e-mail message), via the automated processing of each party’s computer (e.g., by using software or a so-called “electronic agent”), or through human interaction by one party with the other party’s 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 the evidence of these transactions is typically stored on a computer-readable medium, such as a disk, tape, DVD, etc.

Based on the current legislation enacted in the United States and internationally, there are seven key categories of issues that must be addressed in order to conduct a traditional transaction in an electronic

IN THIS ISSUE:

E-Transactions: The Key Rules for Ensuring Enforceability.....	1
From the Editor	2
Social Security Numbers in Commerce: Reconciling Beneficial Uses with Threats to Privacy	13
Implications of Evolving Forms of Exchange Ownership for Their Role as Self-Regulatory Organizations.....	15
Selected Intellectual Property Developments.....	19
Litigation News.....	19
Selected Regulatory Developments	21

WEST
LEGALworks

From the Editor

Few elements of the financial services industry have been as transformed by the revolutions in computer and telecommunications technologies over the past several decades as have securities and futures exchanges. Exchanges are converting to for-profit, public ownership at a blistering pace, and are merging rapidly, across both borders and product lines. As trading efficiency has increased and competition from relatively less regulated alternative trading platforms has intensified, trading costs have plummeted and the types of tradable instruments has exploded, in many cases outstripping the capacity of the exchanges to exercise effective self-regulation and governmental authorities to exercise effective regulatory oversight.

In this issue, Paul Architzel, of Alston & Bird, and formerly chief regulatory counsel for Eurex US and before that chief counsel of what is now the Division of Market Oversight at the Commodity Futures Trading Commission, looks at the evolving forms of ownership of securities and futures exchanges and what this means for the self-regulatory function. The recent move to for-profit, stockholder-owned exchanges has raised difficult issues for both federal and international regulatory authorities, which will only be exacerbated as exchanges continue to merge internationally.

On a different note, Thomas Smedinghoff, of Wildman Harrold, discusses the key rules for ensuring enforceability of e-transactions and the current state of the law, in the United States and the EU, regarding these issues.

Finally, following Experian's article last month on the credit-reporting process, Marc Kirshbaum, president of Experian Fraud Solutions, explains how business-to-business services use Social Security numbers and current federal regulation of these important identifiers.

David E. Brown, Jr., Alston & Bird

Editorial Board

Chairman: John L. Douglas, Alston & Bird LLP

Editor-in-Chief: David E. Brown, Jr., Alston & Bird LLP

Contributing Editors:

Scott A. Anenberg, Mayer, Brown, Rowe & Maw LLP;
Richard M. McDermott, Alston & Bird LLP

Managing Editor: Elizabeth Thompson

David A. Balto
Robins, Kaplan, Miller & Ciresi

Lawrence G. Baxter
President and Chief e-Commerce Officer,
Wachovia Corp.

Roland E. Brandel
Morrison & Foerster LLP

Russell J. Bruemmer
Wilmer Cutler Pickering
Hale & Dorr LLP

Thomas Hal Clarke
Senior Vice President and
Deputy General Counsel,
Wachovia Corp.

Kelly McNamara Corley
Senior Vice President and
General Counsel,
Discover Financial Services,
Inc.

Ellen d'Alelio
Step toe & Johnson

Melanie L. Fein
Goodwin Procter L.L.P.

Paul R. Gupta
Mayer, Brown, Rowe &
Maw LLP

Henry L. Judy
Kirkpatrick & Lockhart LLP

Sylvia Khatcherian
Managing Director, Legal
Department,
Morgan Stanley

C. F. Muckenfuss III
Gibson, Dunn & Crutcher LLP

John C. Murphy, Jr.
Cleary, Gottlieb, Steen &
Hamilton

P. Michael Nugent
Executive Vice President and
General Counsel,
IntelliRisk Management
Corporation

Brian W. Smith
Latham & Watkins LLP

Stuart G. Stein
Hogan & Hartson LLP

Thomas P. Vartanian
Fried, Frank, Harris, Shriver &
Jacobson

Mark A. Weiss
Covington & Burling

Richard M. Whiting
General Counsel and
Executive Director,
The Financial Services
Roundtable

THOMSON
★

Electronic Banking Law and Commerce Report

West Legalworks
395 Hudson Street, 4th Floor
New York, NY 10014

One year subscription, 10 issues, \$372.00
(ISSN: 1090-8420)

Please address all editorial, subscription, and other correspondence to the publishers at west.legalworkspublications@thomson.com

For authorization to photocopy, please contact the Copyright Clearance Center at 222 Rosewood Drive, Danvers, MA 01923, USA (978) 750-8400; fax (978) 646-8600 or West's Copyright Services at 610 Opperman Drive, Eagan, MN 55123, fax (651) 687-7551. Please outline the specific material involved, the number of copies you wish to distribute and the purpose or format of the use.

This publication was created to provide you with accurate and authoritative information concerning the subject matter covered. However, this publication was not necessarily prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional.

Copyright is not claimed as to any part of the original work prepared by a United States Government officer or employee as part of the person's official duties.

environment. They may be summarized by the following questions:

Is the Transaction Authorized in Electronic Form?

Does existing law allow the parties to conduct the transaction in electronic form, or does it present legal barriers that make its enforceability uncertain?

Will the Online Process Result in an Enforceable Contract? Does the online process for entering into a contract support the creation of a valid contract?

Has All Required Information Been Disclosed? Have the parties provided the information or disclosures required by law for the electronic transaction?

Are the Transaction Records Accessible to All Parties? Are copies of the electronic records comprising the transaction available to and capable of being downloaded and printed by all parties?

Has a Valid Electronic Signature Been Used? Have the signature formalities required for this transaction (where applicable) been satisfied with a legally valid form of electronic signature?

Is the Transaction Trustworthy? Has appropriate information security been built into the process in order to ensure the authenticity and integrity of the communications?

Have Appropriate Electronic Record Been Retained? Will the electronic records of this transaction satisfy applicable legal recordkeeping requirements?

This article will consider each of these key questions, and outline the current state of the law with respect to these issues.

1. Is the Transaction Authorized in Electronic Form?

The threshold question for any type of transaction is whether it will be legally valid and enforceable if done in electronic form.² In most cases this involves determining whether applicable law authorizes the transaction to be done in electronic form (or more appropriately, eliminates any legal barriers to doing the transaction electronically).

The general 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, the United Nations, and the governments of numerous other countries have enacted some form of legislation governing the enforceability and conduct of electronic transactions. Generally, such laws support doing most transactions in electronic form.

United States. In the United States, the enforceability of electronic transactions is primarily governed by the Electronic Signatures in Global and National Commerce Act (“E-SIGN”),³ a federal law enacted in

2000 that largely preempts inconsistent state law, and the Uniform Electronic Transactions Act (“UETA”),⁴ 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.⁵

European Union. In the European Union, the enforceability of electronic transactions is governed by the Electronic Signatures Directive adopted in 1999,⁶ the Electronic Commerce Directive adopted in 2000,⁷ and individual country implementations of these Directives.⁸

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”),⁹ which completed work on its Model Law on Electronic Commerce¹⁰ in 1996, and finalized and approved its Model Law on Electronic Signatures in 2001.¹¹ These model laws have served as the basis for legislation enacted in several countries.

International Treaty. The United Nations recently adopted the *United Nations Convention on the Use of Electronic Communications in International Contracts*.¹² 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 signature and 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.

Each of these laws (and many other individual country laws) authorizes most transactions to be conducted in electronic form. They typically do this by providing that the electronic records and electronic signatures that comprise the transactions cannot be denied legal effectiveness solely on the ground that they are in electronic form.¹³ In addition, they often provide 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.¹⁴

The impact of these simple provisions is important, because it prohibits a court from holding that covered transactions are unenforceable solely because of the fact that they are conducted in electronic form. These laws effectively sweep away concerns regarding legal requirements for paper documents and ink signatures.

U.S. and international legislation authorizing the use of electronic records and electronic signatures generally applies to most business, commercial (including consumer),¹⁵ and governmental transactions. 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 instruments¹⁶ and electronic notarization.¹⁷ 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),¹⁸ 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.¹⁹ 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.

But for most transactions, the question is not “whether” you can conduct the transaction in electronic form, but rather “how.”

2. Contracts – Will the Online Process Result in an Enforceable Contract?

Not all electronic transactions involve contracts. But for those that do, the process by which those contracts are created can be critical to enforceability. In the case of electronic transactions that involve agreeing to a *standard form* contracts online (such as click-wrap agreements at a Web site), certain process rules are becoming generally accepted as requirements for ensuring that the contract is enforceable. Specifically, to create an enforceable electronic standard form contract, existing case law in the United States generally requires:

- Clear *notice* to the customer that the transaction is governed by the terms of a contract;
- An *opportunity to review* the terms of the standard form contract before agreeing to them; and
- A clear and unambiguous *statement of what constitutes acceptance* of the terms of the contract.

These requirements are in addition to the standard contract requirement for a signature or other act of assent (e.g., clicking on an “I Accept” button).

2.1 Notice of Existence of a Contract

The first requirement is that the customer must be aware that the transaction is governed by a contract.²⁰ As the Second Circuit pointed out, a customer, “regardless of apparent manifestation of his consent, is not bound by inconspicuous contractual provisions of which he or she

is unaware, contained in a document whose contractual nature is not obvious.”²¹

In the case of the standard click-wrap agreement displayed on a Web site, users have notice of the terms of the agreement when they are presented with all of its terms and required to click “I accept” prior to completing the transaction – e.g., where the contract is displayed within a scroll box, coupled with a statement that it governs the transaction and that the reader should review it carefully. Where this procedure is used, there is generally no question that the customer knows of the contract, and knows that by his or her actions he or she is consenting to its terms.²²

Depending on the method of contract display or reference, however, problems can arise. In fact, inadequate notice of the existence of a contract is one of the major problems with so-called browse-wrap contracts.²³ In one case, for example, the Second Circuit considered a software license made available by link posted in a location on the Web page that a person downloading the software would have no occasion to view (i.e., it was “below the fold”). The court held that “when the writing does not appear to be a contract and the terms are not called to the attention of the recipient . . . no contract is formed with respect to the undisclosed term.”²⁴ In another case, the court dealt with browse-wrap contract terms and conditions at the bottom of the home page that purported to govern use of the Web site. Because the customer need not scroll down to the bottom of the home page and view them in order to proceed to the page of interest, the court found that users were not given proper notice of their existence, and thus their use of the Web site did not constitute consent to them.²⁵

But where properly visible, browse-wrap contracts can be enforceable. In one recent case, for example, the court found that “[t]he statement that the sales were subject to the defendant’s “Terms and Conditions of Sale,” combined with making the “Terms and Conditions of Sale” accessible online by blue hyperlinks, was sufficient notice to the plaintiffs that purchasing the computers online would make the “Terms and Conditions of Sale” binding on them.”²⁶

2.2 Opportunity to Review the Contract

Ensuring that the customer has an opportunity to review the terms of the contract that governs the transaction is also important. *Actual review* of the contract by the customer is not required for enforceability.²⁷ But providing the customer with a reasonable “*opportunity*” to review the agreement is critical.²⁸ Generally, the opportunity to review is construed to include both the actual availability of the contract terms for review, and the right or option to reject the contract and decline to enter into the transaction.

The contract must be “made available in a manner that ought to call it to the attention of a reasonable person and permit review.”²⁹ This means that the customer must at least

have reason to know that the contract terms exist in a form and location that in the circumstances permit review of it or a copy of it. Providing the full text of the contract terms to the customer, such as by using a scroll box, is certainly the best option. But this is often not desirable from a “customer experience” perspective and, due to the limitations of many devices (e.g., PDAs), may not even be practical. Providing a link to the contract terms that is immediately accessible has been held to be acceptable.³⁰

The customer must also have the right to decline to enter into the contract. Otherwise the opportunity to review is meaningless.³¹ For transactions where the opportunity to review occurs prior to a commitment to the transaction, this simply involves ensuring that the customer has the opportunity to decline to proceed with the transaction if he or she finds the terms of the contract unacceptable (e.g., by clicking on a “decline” button or otherwise terminating the process) without incurring any obligation. On the other hand, if the terms of the contract are not available until after there is an initial commitment to the transaction, the case law indicates that ordinarily there is no opportunity to review unless the party can return the product and receive appropriate reimbursement of payments if it rejects the terms.³²

2.3 Specification of Conduct Constituting Acceptance

Creating a contract requires agreement by the parties. The vendor, as master of the offer, may specify the manner or method of the customer’s acceptance, and may propose limitations on the kind of conduct that constitutes acceptance. A buyer may accept by performing the acts the vendor proposes to treat as acceptance.³³ But the method the vendor requires for signifying such agreement should be clear and unambiguous. The customer needs to clearly understand which conduct will evidence agreement to the contract.

In the case of standard click-wrap agreements on a Web site accessed from a PC, this is usually not a problem, as the customer typically must acknowledge the presence of the click-wrap agreement and indicate clear acceptance by clicking on an “I Accept” button in order to proceed with the transaction. Even situations without the use of an “I Accept” button can be sufficient to create a binding agreement, so long as the conduct clearly evidences agreement. In one case, for example, the defendant made its Terms and Conditions of Sale available on its Web site by the use of a blue hyperlink on each of the five Web pages on which the buyer was required to complete online forms in order to purchase the product, and on three of those pages it also included a statement that “All sales are subject to [vendor’s] Terms and Conditions of Sale.” This, the court held, was sufficient to create a binding agreement.³⁴

With a browse-wrap agreement, however, the conduct that constitutes acceptance is frequently as simple as proceeding with the transaction, and can often be done without ever seeing the hyperlink that links to the “terms and conditions” page. In such case, where conduct that constitutes acceptance of the contract is not clearly disclosed to the customer, enforcement is unlikely. In one case, for example, the court held that “[a] consumer’s clicking on a download button does not communicate assent to contractual terms if the offer did not make clear to the consumer that clicking on the download button would signify assent to those terms.”³⁵ The method for signifying assent or rejection should be clear and unambiguous.

In some cases, however, merely accepting the benefits offered by the Web site (with knowledge that the contract exists) can constitute acceptance. As the Second Circuit has pointed out, “it is standard contract doctrine that where a benefit is offered subject to stated conditions, and the offeree makes a decision to take the benefit with knowledge of the terms of the offer, the taking constitutes an acceptance of the terms, which accordingly become binding on the offeree.”³⁶

3. Information Disclosure – Has All Required Information Been Disclosed?

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 law requires the delivery of certain information from vendor to customer as a condition of enforceability. This is frequently (although not always) done as a consumer protection measure. The most important of these provisions are: (1) the requirements that vendors disclose certain information about themselves and/or the transaction, and (2) the consumer disclosure and consent requirements of E-SIGN.

3.1 Vendor E-Transaction Information Requirements

In some electronic transactions, laws requiring disclosure of certain information about the vendor or the transaction itself may be important. 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.³⁷ 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 either: (1) on the first screen displayed when the vendor’s electronic site is accessed, (2) on the screen on

which goods or services are first offered, (3) on the screen on which a buyer may place the order for goods or services, (4) on the screen on which the buyer may enter payment information, such as a credit card account number, or (5) for non-browser-based technologies, in a manner that gives to the user a *reasonable opportunity to review* that information.³⁸

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.³⁹ 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.⁴⁰

3.2 E-SIGN Consumer Information Requirements

A special information disclosure requirement (and corresponding consent requirement) may also apply in certain consumer transactions governed by E-SIGN. This occurs in the limited cases where: (1) a law requires that *information relating to the transaction* be provided to the consumer *in writing*, and (2) the vendor desires to deliver that information to the consumer *electronically*.⁴¹ For example, if applicable law requires financial institutions to deliver monthly statements of account to their customers in writing, and if a financial institution desires to deliver those monthly statements to its customer in electronic form, then the financial institution must make certain information disclosures, and thereafter obtain the consumer's consent to receive those monthly statement electronically. Otherwise the financial institution will be required to continue to send the monthly statements to the consumer on paper.

Specifically, sending the consumer those monthly statements (or whatever information applicable law requires be delivered in writing) in electronic form 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

Failure to make the foregoing disclosures, or failure to obtain the requisite consumer consent, does not invalidate the transaction.⁴⁴ However, the vendor must then provide the requisite information in paper form, or risk being in non-compliance with the applicable rule of law that requires delivery of the information to the consumer in writing.

4. Accessibility – Are the Transaction Records Accessible to All Parties?

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 United States, 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.”⁴⁵

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.”⁴⁶

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

5. Signature – Has a Valid Electronic Signature Been Used?

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, in the United States, 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 U.S. 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 enforceable under U.S. law, both E-SIGN and UETA require that an electronic signature possess three elements:⁴⁷

- 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.⁴⁸

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;⁴⁹
- 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;

- mouse click (such as on an “I Accept” button);⁵⁰
- 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).⁵¹

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.⁵²

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.⁵³

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 the requirements for a valid electronic signature can be somewhat different. Under the EU Electronic Signature Directive, for example, the requirements for a valid electronic signature are: (1) data in an electronic form, (2) attached to or associated with other electronic data, and (3) which serves as a method of authentication.⁵⁴

A third approach to electronic signatures can be found in the recently-approved United Nations Convention on the Use of Electronic Communications in International Contracts. It specifies that legal requirements for a signature will be satisfied if:

- a method is used to *identify* the signer,
- the method is used to indicate the signer's *intention* in respect of the information contained in the electronic document, and
- the method used is either (1) as *reliable as appropriate* to the purpose for which the electronic communication was generated, in light of all the relevant circumstances, or (2) proven in fact to have fulfilled the functions of identifying the signer and indicating the signer's intention.⁵⁵

The signature requirements of the 2005 U.N. Convention go beyond those typically required under U.S. law. In particular, they focus on the issue of security, by requiring the use of a method that (1) *identifies* the signer, and (2) is *reliable*. As such, they highlight the fact that there is a big difference between an electronic signature that merely satisfies the basic requirements of applicable U.S. law (e.g., a mouse click) and a *trustworthy* electronic signature. However, the U.N. Convention does offer an alternative to the reliability requirement, by accepting the use of any method so long as there is a way to prove in fact that it fulfills the functions of identifying the signer and indicating the signer's intention. Thus, presumably even a mouse click could qualify as a signature under the U.N. Convention, but only when done in a way that allows the proponent to ultimately prove "who" clicked, and to establish the intention behind the click.

It is important to note, however, that although clicking a mouse on an "I Accept" button or typing a name on an e-mail message both qualify as legally enforceable signatures in the U.S., they can be problematic. Without more, 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. As a consequence, parties who desire to engage in electronic transactions may find that in some cases merely using a legally compliant electronic signature is not sufficient.

When transactions are automated, and conducted over significant distances using easily altered digital documents, the need for a way to ensure the identity of the sender/signer and the integrity of the document becomes pivotal. Thus, it is 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. There is a clear need for security – for something to ensure that the transaction is trustworthy.

6. Security — Is the Transaction Trustworthy?

Beyond compliance with the statutory requirements for legal enforceability, the primary concern of parties to an electronic transaction 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.

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.⁵⁶

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

6.1 Authentication

In any Internet-based 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.⁵⁷ This requires authenticating 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.⁵⁸ Who created or signed the document? Who sent the message? Is it genuine or a forgery?

A signature *can* be used to authenticate the source of a document. This generally works well with handwritten signatures on paper documents, as such signatures can usually be related to a specific person, through handwriting analysis if necessary. But many 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.⁵⁹ 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. In many respects, it is the legal equivalent of signing a paper contract with an "X". The ultimate question – who typed the name, or who clicked the mouse – often remains unanswered.

Statutes recognizing the legal validity of electronic signatures do not preclude the purported signer from denying that he or she signed a particular electronic document. Just as with ink handwritten signatures, the purported signer is always free to deny that he or she created or authorized the particular electronic signature.⁶⁰ In fact, depending upon the type of electronic signature used, and the level of security inherent in that signature, it is very possible that the electronic signature may be subject to a greater risk of repudiation than a handwritten ink signature. As one court has noted, "a handwritten signature . . . is better evidence of identity than a typed one."⁶¹

This risk must be addressed with security measures appropriate to the transaction. Thus, where inherently weak forms of electronic signature are used (e.g., clicking on an "I Accept" button or typing one's name), it becomes more important to ensure that the person clicking or typing his name has been properly authenticated (e.g., through appropriate secure login procedures or other identity verification procedures), so as to provide an added level of assurance that the signature is valid and properly attributable to a specific

identified person. Alternatively, the use of stronger forms of signature, such as PKI-based digital signatures, may also be appropriate in certain cases.

6.2 Data Integrity

Data integrity is concerned with the accuracy and completeness of information, such as electronic documents and messages communicated over the Internet or stored on the 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."⁶² 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 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.⁶³

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 hash algorithms or cryptographic algorithms, often coupled with digital signatures, is the best way to detect alteration in an electronic document.

7. Record Retention — Have Appropriate Electronic Records Been Retained?

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 record⁶⁴ and;
- remains accessible for later reference.⁶⁵

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.⁶⁶ 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.

Thomas J. Smedinghoff (smedinghoff@wildmanharrold.com) is a partner at the law firm of Wildman Harrold, in Chicago (www.wildmanharrold.com). 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 was also 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) that wrote the Illinois Electronic Commerce Security Act (5 Ill. Comp. Stat. 175).

1. See UN Press release at <http://www.un.org/News/Press/docs/2005/ga10424.doc.htm>. A copy of the 2005 *United Nations Convention on the Use of Electronic Communications in International Contracts* is available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html.
2. 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.
3. 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.
4. 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.
5. As of May 1, 2006, 46 states and the District of Columbia had enacted UETA. For an updated list of those states that have enacted UETA, see www.nccusl.org/nccusl/uniformact_factsheets/uniformacts-fs-ueta.asp.
6. 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 http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf.
7. 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 www.europa.eu.int/ISPO/e-commerce/legal/documents/2000_31ec/2000_31ec_en.pdf.
8. 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/europe/2005/all_about/security/electronic_sig_report.pdf.
9. 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 www.uncitral.org.
10. 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
11. See United Nations, UNCITRAL Model Law on Electronic Signatures 2001, available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html.
12. See UN Press release at <http://www.un.org/News/Press/docs/2005/ga10424.doc.htm>. A copy of the 2005 *United Nations Convention on the Use of Electronic Communications in International Contracts* is available at http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html.

13. E-SIGN, 15 U.S.C. § 7001(a) ; UETA § 7(a) ; Electronic Signature Directive, Article 5(2); United Nations Convention on the Use of Electronic Communications in International Contracts, Article 8(1). See also UNCITRAL Model Law on Electronic Commerce, Articles 5, 6, and 7.
14. See, e.g., UETA §§ 7(c) and 7(d).
15. The United Nations Convention on the Use of Electronic Communications in International Contracts, however, excludes consumer transactions from its scope. Article 2(1)(a).
16. See, E-SIGN, 15 U.S.C. § 7008, and UETA § 16.
17. See, E-SIGN, 15 U.S.C. § 7001(g), and UETA § 11.
18. 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).
19. See, E-SIGN, 15 U.S.C. § 7003, and UETA § 3(b) for a complete list of exceptions.
20. *Specht v. Netscape Communications Corp.*, 306 F.3d 17, 34, fn 16 (2d Cir. 2002) (the court described this as “the principle of conspicuous notice of the existence of contract terms”).
21. *Specht*, 306 F.3d at 29 (applying California law and finding that an individual downloading software was not bound by terms purporting to govern the transaction because he was not made aware that he was entering into a contract by the act of downloading).
22. *Microstar v. Formgen*, 942 F. Supp. 1312, 1315, 1317 (S.D. Cal. 1996) (contrasting this traditional process with the facts before it, where the only reference to the existence of a license agreement was in the opening screen for the build editor for a game that said “please refer to LICENSE.DOC for further information on levels created with BUILD.EXE.”)
23. A “browse-wrap agreement” is an online agreement that appears on a Web site (usually via a link), but does not require the user to take any action to express consent to its terms, other than e.g., merely continuing to use the Web site.
24. *Specht v. Netscape Communications Corp.*, 306 F.3d 17, 30 (2d Cir. 2002). In that case, the court found that “where consumers are urged to download free software at the immediate click of a button, a reference to the existence of license terms on a submerged screen is not sufficient to place consumers on inquiry or constructive notice of those terms.” *Specht* 306 F.3d at 32. But see *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 401-403 (2d Cir. 2004) (holding that contract terms that were not displayed to the Web site visitor until after the visitor obtained the benefit sought would nonetheless apply where visitor made daily visits to the site to obtain continued information with full knowledge of the terms imposed by Web site operator); and *Cairo, Inc. v. Crossmedia Services, Inc.* No. C 04-04825 JW (ND Cal. April 1, 2005) (citing *Register.com* for proposition that knowledge of Web site’s terms and conditions can be imputed to a party that uses a software robot or crawler to repeatedly visit a Web site).
25. *Ticketmaster Corp. v. Tickets.com, Inc.*, 54 U.S.P.Q.2d (BNA) 1344 (C.D. Cal. 2000).
26. *Hubbert v. Dell Corporation*, 835 N.E.2d 113, 122 (Ill. App. 2005).
27. See *James v. McDonald’s Corporation*, 417 F.3d 672 (7th Cir. 2005), *Hill v. Gateway 2000, Inc.*, 105 F.3d 1147, 1148 (7th Cir. 1997) (“A contract need not be read to be effective; people who accept take the risk that the unread terms may in retrospect prove unwelcome. *Carr v. CIGNA Securities, Inc.*, 95 F.3d 544, 547 (7th Cir. 1996); *Chicago Pacific Corp. v. Canada Life Assurance Co.*, 850 F.2d 334 (7th Cir. 1988)”); *Groff v. America Online, Inc.*, 1998 WL 307001 (R.I. Super. May 27, 1998) (noting “the general rule that a party who signs an instrument manifests his assent to it and cannot later complain that he did not read the instrument or that he did not understand its contents.”); *Specht v. Netscape Communications Corp.*, 306 F.3d 17, 30 (2d Cir. 2002) (“It is true that [a] party cannot avoid the terms of a contract on the ground that he or she failed to read it before signing.”)
28. See, e.g., *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447 (7th Cir. 1996), which held that terms inside a box of software bound consumers who use the software after an opportunity to read the terms and to reject them by returning the product, and *Hill v. Gateway 2000, Inc.*, 105 F.3d 1147, 1148 (7th Cir. 1997).
29. *Specht*, 306 F.3d at 30.
30. *Hubbert v. Dell Corporation*, 835 N.E.2d 113 (Ill. App. 5th Cir. 2005); *DeJohn v. The .TV Corp. Int’l*, 245 F. Supp. 2d 913 (N.D. Ill. 2003).
31. *ProCD*, 86 F.3d at 1451; *Hill v. Gateway 2000, Inc.*, 105 F.3d 1147, 1148 (7th Cir. 1997).” *I. Lan Systems v. Netscout Service Level Corp.*, 183 F. Supp 2d 328, 337-8 (D. Mass. 2002).
32. *Sun Trust Bank v. Sun International Hotels Ltd.*, 184 F. Supp. 2d 1246 (S.D. Fla. 2001).
33. *Specht v. Netscape Communications Corp.*, 150 F. Supp. 2d 585, 591-2 (S.D.N.Y. 2001), *aff’d*, 306 F.3d 17 (2d Cir. 2002). *ProCD* 86 F.3d at 1452 and *Hill v. Gateway* 105 F.3d at 1149.
34. *Hubbert v. Dell Corporation*, 835 N.E.2d 113 (Ill. App. 5th Cir. August 12, 2005).
35. *Specht v. Netscape Communications Corp.*, 306 F.3d 17 (2d Cir. 2002)
36. *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 403 (2d Cir. 2004).
37. California Business & Professions Code, Section 17538(d).
38. California Business & Professions Code § 17538(d)(2)(A).
39. Electronic Commerce Directive, Article 10(1).
40. Electronic Commerce Directive, Article 11(1) and 11(2). The United Nations Convention on the Use of Electronic Communications in International Contracts 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 United Nations Convention on the Use of Electronic Communications in International Contracts, Article 7.
41. See E-SIGN, 15 U.S.C. § 7001(c).
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).
44. E-SIGN, 15 U.S.C. § 7001(c) (3).
45. E-SIGN, 15 U.S.C. § 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.”)
46. Directive 2000/31/EC (Electronic Commerce Directive), Article 10(3).
47. E-SIGN, 15 U.S.C. § 7006(5) and UETA § 2(8) (definitions of “electronic signature”).
48. See UETA §§ 2(8) and 7(d) and E-SIGN, 15 U.S.C. § 7001(a) and 7006(5).
49. See, e.g., *Rosenfeld v. Zern*, 2004 N.Y. Slip Op. 24143 (2004); *Shattuck v. Klotzbach*, 2001 WL 1839720 (December 11, 2001)
50. 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).
51. 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).
52. See UETA, Section 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 requires 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.”
53. See, for example, *Parma Tile Mosaic & Marble Co. v. Estate of Fred Short 2 No. 20*, 1996 WL 73828 (N.Y. Ct. App. Fed. 20, 1996). See also *Kohlmeyer & Co. v. Bowen*, 126 Ga. App. 700, 192 S.E.2d 400 (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).
54. EU Electronic Signature Directive, Article 2(1). The EU also recognizes another type of electronic signature known as an “Advanced Electronic Signature.” An Advanced Electronic Signature is considered to be more secure, and thus enjoys greater legal acceptability. If a signature meets the requirements of an electronic signature, it will also qualify as an advanced electronic signature if it is: (1) uniquely linked to the signatory, (2) capable of identifying the signatory, (3) created using means that the signatory can maintain under his sole control, and (4) is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable. EU Electronic Signature Directive Article 2(2).
55. United Nations Convention on the Use of Electronic Communications in International Contracts, Article 9(3).
56. 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.
57. See, e.g., IRS Announcement 98-27, Paragraph (1)
58. 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. § 3532(b)(1)(D).
59. 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.
60. See, e.g., *In re Piranha, Inc.*, 297 B.R. 78 (N.D. Tex. June 20, 2003), *Aff’d*, 33 Fed. Appx. 19 (5th Cir. Dec. 9, 2003) (noting that UETA “does not preclude a person from contesting that he executed, adopted, or authorized an electronic signature that is purportedly his”).
61. *Cloud Corporation v. Hasbro, Inc.*, 314 F.3d 289, 296 (7th Cir. Dec. 26, 2002).
62. Homeland Security Act of 2002 § 1001(b), amending 44 U.S.C. § 3532(b)(1)(A).
63. See, e.g., *Victory Med. Hosp. v. Rice*, 493 N.E.2d 117 (Ill. App. Ct. 1986).
64. 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).
65. 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.
66. E-SIGN 15 U.S.C. § 7001(d)(3); UETA § 12(d).