USING ELECTRONIC RECORDS AND SIGNATURES IN FACE-TO-FACE TRANSACTIONS UNDER THE UNIFORM ELECTRONIC TRANSACTIONS ACT AND THE ESIGN ACT[1] —

AN EVALUATION OF THE INTERLINK ELECTRONICS ePAD™

A White Paper

R. David Whitaker
Of Counsel
Goodwin | Procter LLP
March 20, 2001

---

1. This White Paper is published to provide a summary of significant developments and for purposes of education and discussion. It is intended to be informational only and does not constitute legal advice regarding any specific situation or product. Product features have not been verified and no endorsement of any product or service by the author is intended or implied. The views expressed are those of the author and not of any other person.

INTRODUCTION

On July 29th, 1999, the National Conference of Commissioners on Uniform State Laws (NCCUSL) gave final approval to the Uniform Electronic Transactions Act (UETA). The UETA is a response to the myriad state laws regulating commerce that assume, or require, the existence of paper documents and handwritten signatures as a precondition to the enforcement of commercial rights. The UETA is a statutory "overlay." It sets up uniform rules for revising traditional writing and signature requirements in the law to permit the use of electronic records and electronic authentication methods. Although there are some exclusions and exceptions to the new rules, in general the UETA's coverage is very broad and reaches most business and consumer transactions, including those involving real estate, mortgages, insurance, and consumer disclosures governed by state law.

To date, 24 states have enacted the UETA. However, some states adopting the UETA have changed the statute to reflect local preferences or policies, producing non-uniform versions. Other states currently have unique state laws, other than the UETA, that govern the general use of electronic records and signatures. In response to concerns over non-uniform state laws, and the need to address writing and signature requirements in federal law, Congress passed the federal Electronic Signatures in Global and National Commerce Act. President Clinton signed the Act in late June of 2000, and most of ESIGN's provisions became effective as of October 1, 2000. The E-SIGN Act adopts most of the UETA's principal provisions, creating federal "baseline" rules for electronic records and signatures. The E-SIGN Act covers federal law and also covers those states that have not enacted either (i) the Official Text of the UETA or (ii) an equivalent law that is consistent with ESIGN. It establishes certain additional consumer protections beyond those in the UETA, and limits the ability of states to vary or alter the baseline rules.

This paper addresses the application of the UETA and ESIGN to electronic records and signatures used in connection with face-to-face transactions, and evaluates one potential method of obtaining an electronic signature in such instances.

POTENTIAL APPLICATIONS IN FACE-TO-FACE TRANSACTIONS

The potential impact of electronic records and signatures has been widely misunderstood, and underestimated. Many commentators and analysts have focused on the use of electronic signatures and records for remote transactions occurring over the Internet or some other type of electronic network. While these applications are valuable, they are by no means exclusive. The primary economic benefit of substituting electronic records and signatures for traditional paper-and-ink documents is not the ability to execute documents remotely; it is the ability to better manage data, workflow, quality control, speed of delivery, and document management (storage, retrieval and transmission). These benefits are available whether a transaction is initiated online, or in person.

There are a wide variety of face-to-face transactions that could reap potential benefits from the use of electronic records and signatures. The UETA and ESIGN, when combined with the electronic record and signature rules of other new uniform laws (such as Revised Article 9 of the Uniform

Commercial Code, covering secured transactions in goods), would permit the use of electronic records and signature in most significant business and consumer sales, service, licensing, lending and leasing transactions. Here are just a few examples:

- **Automobile loans and leases**. Today, many automobile purchasers obtain their financing at the dealership. The dealer, in turn, sells the loan to one of several financing sources and forwards the loan documentation for review and acceptance. Under ESIGN, the UETA and Revised Article 9 of the UCC, the loan documentation could be electronically signed, stored, and delivered from the dealer to the financing company, which could then automate most of its review, quality control and acceptance process.
- **Insurance applications**. Both consumers and businesses seeking insurance coverage are frequently required to complete and sign applications providing the insurance company with information used in evaluating the risk. These applications are often signed in the office of an independent agent or a representative of the insurance company. Use of an electronic application and signature could streamline the process of taking in and evaluating the application, and issuing the policy.
- **Mortgage loan documentation**. Mortgage loan transactions, whether involving residential or commercial property, involve large numbers of disclosures, submission of documents from a variety of parties, and a complex document closing process. Because of requirements for notarization and (in some states) witnessing of signatures, it is probably that many of these transactions will continue to require in-person closings. In addition, applications for commencing the mortgage loan process are often taken in person by brokers and lenders. ESIGN and the UETA make it possible for virtually all the documents associated with a mortgage loan to be prepared, signed, stored and managed electronically. The potential improvements electronic records and signatures offer for quality control, speed of processing and sale into the secondary market, and information delivery and management in these transactions are immense.

Underlying Goals

The UETA and ESIGN were drafted with a specific set of goals and policy choices in mind. Understanding the goals and policies that underlie the UETA and ESIGN is essential to understanding the two statutes.

First and foremost, the UETA and ESIGN are intended to level the legal "playing field" between paper-based documents and other information storage and communication technologies. They recognize the many legal purposes writings serve, including the following:

- Memorializing agreements
- Communicating information
- Preserving information for later reference
- Providing notice
- Undertaking obligations
- Transferring rights
- Confirming information

The UETA and ESIGN create a system of ground rules that preserve and further these purposes in an electronic environment, providing enhanced certainty and legal protection for parties wishing to use electronic records in place of writings.

Second, the UETA and ESIGN establish technologically neutral rules. They do not enshrine any particular methodology or technology solution. Electronic records may take a wide variety of forms, and may be retained on any commercially viable storage media. Electronic signatures may be anything from a simple typed symbol to a complex, highly secure system of encryption. Rules for record access do not presume a particular access method or file format. The possibilities are limited only by the basic policy choices in the two statutes and the imagination of systems designers.

Third, the UETA and ESIGN are minimalist procedural statutes. They do not attempt to provide a complete regulatory scheme, with detailed rules covering as many anticipated permutations and special situations as possible. Instead, they recognize the inherent flexibility and adaptability of the common law, and also the wide variety of substantive statutes that already exist and will be just as applicable to electronic records as they are to written documents.

The Three General Rules

Under ESIGN and the UETA, the following three general rules apply:

- A record or signature may not be denied legal effect or enforceability solely because it is in electronic form;
- 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. UETA § 7; ESIGN § 101(a).

These three general rules, in turn, are built upon three defined terms: record, electronic record, and electronic signature.

A "record" under the UETA and ESIGN is "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form." UETA § 2(13); ESIGN § 106. This encompasses not only traditional writings, but also anything which is stored on magnetic or optical media (such as a computer hard drive or CD-ROM). Essentially, all that is required is that the information is stored and may be retrieved for review. There is no requirement as to where storage physically occurs. For example, if an individual uses the Internet to review information stored on a server two thousand miles away, that information is still a record. The requirement that the record be "retrievable in perceivable form" is an objective, and not subjective, requirement. To qualify, it is not necessary that the specific recipient be able to comprehend the information contained in the record, just that *someone* could comprehend it. For example, a data file stored on a hard drive which displays information in Spanish is a record for purposes of the UETA, even if the person reviewing the record does not speak Spanish.

An "electronic record" under UETA and ESIGN is "a record created, generated, sent, communicated, received, or stored by electronic means." UETA § 2(7); ESIGN § 106. Essentially, the term is intended in all three statutes to cover any type of record which is generated or stored electronically; as such, it would cover records created on a computer and stored on any type of media.

An "electronic signature" under UETA and ESIGN is an "electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record." UETA § 2(8); ESIGN § 106. Included within this definition would be traditional ink signatures, typed names, or a click-through on a software program's dialog box combined with some other identification process, biometric measurements (such as a retina scan or thumbprint), a digitized picture of a handwritten signature, or a complex, encrypted authentication system. As with a traditional ink signature, the legal consequences of the signature, and the question of whether the signature may properly be attributed to a particular person, is left to other law and the surrounding factual circumstances.

It is particularly important to note the use of the term "process" in the definition. This means that the creation of an electronic signature may involve multiple steps and consideration of surrounding circumstances. For example, as part of a contract execution, assume that a consumer appears at the seller's offices, where his identity is verified by reference to his driver's license and

other identification. The customer is then placed in front of a computer with a signature pad, where he signs his name using the pad and a stylus. The graphic image created by the pad is appended at the end of an electronic form contract intending to signify acceptance of the contract terms, and the seller also notes on the form the steps taken to identify the consumer. The entire procedure, including the verification of identity and the affixing of the name to the contract, would constitute a "process" resulting in an electronic signature.

As another example, assume that a financial institution requires that each customer using its Internet Banking site for the first time must enter the sixteen digit number from the customer's ATM card plus the associated secret PIN, and is then presented with a copy of the institution's Internet banking agreement together with an accompanying dialog box indicating the customer's assent to the agreement's terms. The customer is required to affirmatively "click-through" the dialog box, affirming consent to the agreement's terms, before accessing the on-line banking services. The combination of the identification process plus the "click-through" would constitute an electronic signature.

Contested Signatures

The UETA and ESIGN do not change the existing common law rules concerning contested signatures and the burden of proof. If the authenticity of an electronic signature is in dispute, the person seeking to enforce the signature will be required to prove that the signature was executed by the person against whom enforcement is sought. This means that parties accepting electronic signatures will need to be satisfied that the signature is sufficiently verifiable, under the circumstances and for the contemplated purpose, to counterbalance the risk of such a dispute.

Intent to Sign

The UETA and ESIGN both retain the existing requirement that a signature is only valid if the signer intends to sign something. UETA § 2(8); ESIGN § 106. Currently, a number of conventions are used with written documents in order to provide evidence of the intent to sign - placement of the signature at the end of the document, statements above the signature that the parties are signing the document to demonstrate their agreement to the terms in the document, notarized acknowledgments of the signature, etc. The act of signing itself – taking up the pen, subscribing a name to the document in a specified place – serves in its own right as evidence of the intent to sign because the ceremony is an ingrained part of our culture. Because the requirement of an intention to sign is built into the definition of electronic signature under both statutes, parties hoping to enforce signed records at a later date should include a certain amount of ceremony as part of the online signing process; failing to do creates the risk of a later claim that there was no intent to sign, and therefore no signature.

As with existing law, the purpose the signature serves is left to other law and the surrounding factual circumstances. The signature may serve any of several purposes:

- Confirming the accuracy of the document;
- Confirming receipt or review of the document; or
- Confirming agreement with the document's terms.

The UETA and ESIGN make no attempt to distinguish between these different uses for a signature, or to set different standards of proof or attribution depending on the signature's purpose.

Special Rules for Electronic Records

While the UETA and ESIGN set up no special standards for the use of electronic signatures, they do have a number of special rules for electronic records that are intended to substitute for certain types of writings. For example:

- If a person is required by law to provide or deliver information in writing to another person, that requirement is only satisfied by an electronic record if the recipient may keep a copy of the record for later reference and review. If the sender deliberately inhibits the recipient's ability to print or store the record for later review, then the record doesn't satisfy the legal requirement that the information be provided or delivered. UETA § 8(a); ESIGN § 101(e).
- If a particular writing is required by law to be displayed in a particular format, the UETA and ESIGN do not change that requirement. For example, if current law requires a notice to be printed in at least 12 point type and a boldface font, that requirement remains in place under the UETA. If the law requires two elements of a document to be placed in a particular physical relationship to each other or some other part of the document, that requirement also is not changed by the UETA. UETA § 8(b); ESIGN § 101(b)(1). For example, if the law requires a disclosure to be displayed just above a contracting party's signature, that rule must be observed within the electronic record.
- Electronic records that represent binding obligations (such as a contract, lease or security agreement) are only enforceable against a recipient if the sender does not inhibit the recipient's ability to store or print the record. UETA § 8(c); ESIGN § 101(e).

Generally speaking, these rules are not variable by agreement; however, if the underlying statutory requirement that information be delivered in writing, or by a particular delivery method, may be varied by agreement, then the requirement that an equivalent electronic record be capable of storage, or be delivered by the same method as a writing, may also be waived.

Neither ESIGN nor the UETA change any requirements concerning timing of delivery of disclosures and notices, or any requirements concerning the placement or formatting of required notices or disclosures. For example, if a state insurance regulation requires a disclosure to be made in a minimum of 12 point type directly above the document's signature lines, capitalized and boldface, that requirement must be met when delivering the notice or disclosure electronically.

THE INTERLINK ePAD™ — AN EVALUATION

Interlink Electronics, Inc., offers an electronic signature pad, called the ePad, for capturing a handwritten signature electronically and embedding it in electronic records. The ePad is described as using a semi conductive input pad that captures pen input along both the X and Y-axes and discriminates 128 levels of pressure (applied with a common stylus) along the Z-axis. As described, the ePad is suitable for both straight capture of a handwritten signature as a graphic and for biometric applications, where signature characteristics may be used to facilitate verification of identity. Interlink has paired the ePad with a variety of electronic signature software solutions. The ePad is used as the equivalent of the signature line on a piece of paper – the signer writes his or her signature in the usual way on the pad, and the signature itself, together with the biometric data, is captured and embedded into the document. The signature can be displayed on the electronic record in the same way that a handwritten signature would appear on paper. The embedded information, although not visible, becomes part of the document.

A device like the ePad is well suited to the purpose of creating electronic signatures in face-to-face transactions. To begin with, an ePad signature should provide substantial evidence of the intent to sign the document. The signature process utilized, including the surrounding ceremony, is familiar to most people. The signature may be placed in a recognizable signature block in the record in the same location where one would sign an equivalent paper document. When paired with a well-designed system for presenting the documents, it should be difficult for most people using the ePad to make a credible claim that they did not understand that they were creating a signature.

In the case of a dispute over the authenticity of the signature, a good argument can be made that an ePad signature is no worse as evidence, and may be better, than an ink signature. In many cases, proof of authenticity currently centers, not around the signature itself, but around the surrounding circumstances of the transaction and the actions of the parties. With an ePad signature, the surrounding circumstances and actions of the signer will often be virtually identical to the equivalent paper transaction. In other words, the process of signing, and the people present to observe the signing, will be the same. The signature process itself will be comprehensible to third parties without an extended explanation of the technology. Courts and juries will find themselves in familiar territory. Of course, traditional handwriting analysis, which relies on an exacting evaluation of signature characteristics using multiple original samples, will probably not be usable in authenticating an electronic signature (although it is conceivable that the captured biometric information in an ePad signature might someday be of use to a new breed of handwriting experts). But as anyone who has engaged in the exercise can attest, handwriting analysis is often inconclusive and the subject of conflicting expert testimony.

In cases where full advantage is taken of the ability to make biometric measurements, an ePad signature may actually be an improvement over a handwritten signature. Software taking biometric measurements of signatures can be set to varying thresholds of certainty concerning the "match" between the electronic signature associated with the record and a reference signature for the signer. If a reference signature has been obtained and stored, the software may be set at a level sufficiently discriminating that it should provide a substantial level of comfort that the two signatures were executed by the same person. In the same vein, an ePad signature integrated into a

biometric testing process may have advantages over other types of digital identification, such as dual-key encryption, for establishing reasonable certainty of identity. The use of an encryption key is only as secure as the signer's protection of the key – if the key is held on a smart card and applied by entering a six-digit PIN that the signer keeps taped on the card, then the key is not really all that secure. Biometric measurements are harder to misappropriate, and do not require the signer to store and carry a device bearing the key.

An ePad signature should also be highly compatible with the UETA and ESIGN requirements for record access and formatting. If the customer wishes to receive a paper copy of the record, it can be printed with a graphic representation of the signature, located in the same place an ink signature would appear. The function of the signature should be as readily apparent as on a paper equivalent. Furthermore, the signature will appear on the customer's copy as it appears in the operative record kept by the other party. The clear placement of the signature on the record should also give comfort concerning compliance with laws that require notices and disclosures to be placed in a particular juxtaposition to the signature line. These advantages are not necessarily present with some other types of electronic signature, where the signature is less an object than a process and may not be visible on the electronic record at all.

It should be noted that the effectiveness of an ePad signature, whether or not integrated into a biometric testing process, is dependent on the surrounding system for creating, storing, managing, and retrieving the electronic records associated with the signature. In order for the signature to be effective, it must be possible to demonstrate that the signature is associated with the correct record, has not been misappropriated for use on other records by replication, and that the associated electronic record has been not been altered since it was signed. Assuming that these and other legal criteria are met, the ePad should prove an effective tool for obtaining an enforceable electronic signature in many consumer and business-to-business applications.