SUTHERLAND

Overview of the U.S. E-Sign Act and the Uniform Electronic Transactions Act and Practice Points for Using Electronic Records and Signatures

Legal Framework

Federal Law: Electronic Signatures in Global and National Commerce Act (E-Sign Act) became effective on October 1, 2000.

State Law: Forty-seven states have adopted a version of the Uniform Electronic Transactions Act (UETA). Illinois, New York and Washington have not adopted UETA but have their own electronic transaction acts.

Overview of the Law

Both the E-Sign Act and UETA provide that (i) a record or signature cannot be denied legal effect, validity or enforceability solely because it is in electronic form, (ii) if law requires a record to be in writing, an electronic record can satisfy the requirement, and (iii) a contract cannot be denied legal effect, validity or enforceability solely because an electronic signature was used in its formation.

Under both the E-Sign Act and UETA, parties to a transaction are not required to agree to use or accept electronic records or electronic signatures. Agreement to the use of electronic records and signatures will be construed broadly, though, and may be established based on the parties' conduct. However, obtaining a written agreement to use electronic records and electronic signatures is a simple and failsafe practice to evidence the parties' intent.

What is an Electronic Signature?

An "electronic signature" under the E-Sign Act and UETA means an electronic sound, symbol or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record. Examples of electronic signatures include a scanned or digitally captured image of a manual signature, a click to "accept and sign" button on a webpage or mobile application, or a signature signed into an electronic record using the mouse or a stylus on a touchscreen.

What is a Digital Signature?

A digital signature or digital certificate is a type of cryptography that can be used to authenticate the sender of an electronic record through use of private and public keys. As such, a digital signature can be used as a specific type of electronic signature (but not all electronic signatures are digital signatures). In simple terms, when using a digital signature, the document is encrypted using a private key assigned to, and accessible only by, the signing party when the document is sent by the signer to the recipient. The recipient then uses a public key also assigned to the signing party to decrypt the document. The document encrypted with the signer's private key can only be decrypted using the signer's public key (and conversely, the signer's public key can only decrypt files that have been encrypted with the signer's private key). So if the public key is able to decrypt the document, it proves that the signing party sent the document and that the document has not been altered in transit. As such, the digital signature verifies the signer as the source of the document.

Consumer Consent and Disclosure Requirements

Under the E-Sign Act, if an electronic record is used in a transaction with a consumer, the following consent and disclosure requirements must be satisfied:

- The consumer must consent to the use of the electronic record. The consent must be obtained or confirmed electronically in a manner that reasonably demonstrates that the consumer can access the information in the electronic form to be used.

- Prior to obtaining the consent, the consumer must be provided with a clear and conspicuous statement of:
    - Whether the consent applies only to the particular record at issue or to identified categories of records;
    - The consumer's right to withdraw his or her consent to the use of electronic records, and the process for withdrawing consent;
    - Any conditions, consequences or fees resulting from the withdrawal of consent to the use of electronic records;
    - The procedure for the consumer to update his or her contact information;
    - The consumer's right to receive the record in non-electronic form;
    - How the consumer can request and obtain a paper copy of an electronic record, and whether a fee will be charged; and
    - The hardware and software requirements for access to and retention of the electronic records.

- If there is a subsequent change in hardware or software requirements that creates a material risk that the consumer will not be able to access or retain the electronic records:
    - The consumer must be provided with a statement of the new hardware and software requirements;
    - The consumer must be informed of his or her right to withdraw consent to further use of electronic records without any fees; and
    - The consumer's consent to the use of electronic records should be reconfirmed in a manner that reasonably demonstrates that the consumer can access the information under the new requirements.

Exceptions to the E-Sign Act and UETA

Neither the E-Sign Act nor UETA apply to (i) laws governing wills, codicils and testamentary trusts, or (ii) the Uniform Commercial Code, other than Articles 2 (sale of goods) and 2A (leases) thereof.

The following are also excepted from the E-Sign Act (but not from UETA): (i) records governed by state laws on adoption, divorce or other family law matters; (ii) official court documents and court orders; (iii) notice of cancellation of utility services; (iv) notice of default, foreclosure or eviction under credit agreements secured by, or rental agreements for, a primary residence; (v) notice of cancellation of health or life insurance coverage or benefits; (vi) product recalls; and (vii) documents required to accompany handling of hazardous substances.

These exclusions do not mean that electronic records or electronic signatures are, per se, not valid for these types or records, but you will need to look to the bodies of law that govern those types of records to determine whether or not electronic records and/or signatures can be used.

Practice Points

- Consider including an express agreement to the use of electronic records and electronic signatures in the agreement itself or in the e-sign workflow, such as building it as a click-through feature when accessing or electronically signing the online contract.
    - Sample clause: "*The parties agree that this Agreement and all notices and disclosures made or given in connection with this Agreement may be created, executed, delivered and retained electronically. As such, the parties agree that this Agreement and any related documents may be signed electronically, and that the electronic signatures appearing on this Agreement or any related documents shall have the same legal effect for all purposes, including validity, enforceability and admissibility, as a handwritten signature.*"

- Give the counterparty the ability to opt out of the use of electronic records and signatures, and notify the counterparty how it can opt out and instead sign manually. This may be required in the case of transactions with consumers.

- For transactions with consumers, provide the required notices and disclosures for consumers (summarized above) prior to signing, and obtain or confirm the consumer's consent to the use of electronic records and electronic signatures in a manner that reasonably demonstrates his or her ability to access the information. For example, if the consumer's consent is obtained through the same application or file format (e.g., PDF) that will be used for the electronic records, then this requirement should be satisfied.

- Consider what level of identity authentication to be used. Alternatives could include:
    - In the event of a negotiated transaction, exchanging signed documents by representatives of each party who are known to the other party via email;
    - Sending a link that accesses the electronic contract to a verified email address with a process to confirm that the electronic contract was then accessed and signed via that link;
    - Requiring the counterparty to create and sign into an account with a username and password to access the electronic record;
    - Requiring the counterparty to scan a picture of his or her photo ID and attach it to the electronic contract file;
    - Using knowledge-based authentication that requires the counterparty to prove his or her identity by answering questions unique to him or her (such as prior addresses, phone number, mother's maiden name, or pre-established security questions). These data points could be collected from the consumer upon account creation or pulled from public databases;
    - Two-factor authentication where the counterparty is required to enter a code that is delivered to him or her via phone call, text message or email; and/or
    - Using a digital signature.

  The level of authentication used may depend on factors such as the sensitivity or value of the contract, the risk tolerance of the parties, and the likelihood of fraudulent activity or repudiation. This determination will also need to balance the desire for security against the commercial need for ease of use.

- Create an audit trail. When planning the workflow for the e-signing process, consider what data points can be created and retained to verify and authenticate that the document was signed, how and when the document was signed, and that the document has not been modified from the version that was signed. For example, the audit trail data points could include the date the document was sent to the counterparty and by whom, the date and time the document was signed, the email

address or IP address used by the recipient to access and/or send the signed document, other identity authentication methods used to access and sign the document, and the method to verify that the document has not been modified.

- Provide the counterparty with a copy of the fully executed document promptly after the document is electronically signed and accepted.

- Retain a complete and accurate copy of the electronic record in a format that can be accessed and retrieved. Consult your company's document retention policy and ensure that you retain electronic contracts in other records in accordance with that policy. Also retain any audit trail created in the e-signing process to verify that the record was signed and is an accurate and unmodified version of the record that the counterparty signed.

For more information, please contact:

Bob Pile	404.853.8487	robert.pile@sutherland.com
Brian Murphy	404.853.8178	brian.murphy@sutherland.com