Electronic Signature Law in the U.S.

WHITEPAPER

10.06.20

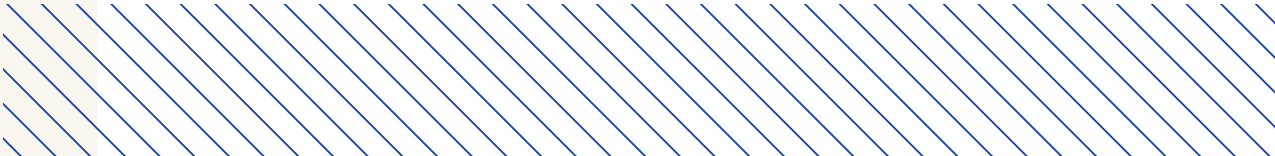
Filevine

Overview

DISCLAIMER: This is a general overview of electronic signature law in the U.S. as it stands at the time of the creation of this document. Because laws frequently change and because this document is not intended as legal advice, please consult an attorney before relying on any information provided.

An electronic signature (e-signature) is any electronic process that indicates acceptance of an agreement or record. Legislation defines an e-signature as “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 e-signatures include entering a password or PIN, typing a name, responding to telephone keypad instructions, clicking a button or checkbox, or responding to an email thread in a manner that manifests assent.

While the U.S. has several different acts dictating the use and interpretation of e-signatures, the laws are similar in effect, and there is considerable consensus on the appropriate standard to comply with e-signature law. The Electronic Signatures in Global and National Commerce (ESIGN) Act, signed into law in 2000, made e-signatures legal in the federal arena. The Uniform Electronic Transactions Act (UETA) is the state counterpart to ESIGN and has been adopted by every state except Illinois, New York, and Washington. These three states have their own e-signature laws. Fortunately, because of the similarities in all of the e-signature legislation, most businesses are able to use a single process for e-signatures country-wide.



ESIGN

The ESIGN Act gave e-signatures equal legal footing to handwritten signatures federally. ESIGN 1) ensures that any law that requires a signature may be satisfied by an electronic signature, 2) allows electronically executed agreements to be presented as evidence in court, and 3) prevents denial of legality, validity, or enforceability of an e-signed document solely on the basis of it being in electronic form. ESIGN is neutral about the type of technology used; it preempts state laws that proscribes specific technology. In fact, ESIGN preempts any state law not consistent with it. However, state laws adopted from UETA are not preempted, unless they contain exceptions that are inconsistent with ESIGN. Case law on ESIGN has consistently confirmed its broad effect, as ESIGN applies to "any transaction in or affecting interstate commerce." It should be noted that ESIGN does not apply to all contracts and documents. For example ESIGN does not apply to wills, codicils, and testamentary trusts. It also does not apply to adoptions, divorce, or other matters of family law, as well as certain sections of the Uniform Commercial Code.

The ESIGN Act ensures that any law that requires a signature may be satisfied by an electronic signature.

UETA

Similar to ESIGN, UETA prevents denial of a record or signature simply because it's electronic. Additionally UETA specifies that 1) a contract cannot be denied legal effect of enforceability simply because an electronic record was used in its formation, 2) an electronic record satisfies the legal requirement for a record to be in writing, and 3) an electronic signature satisfies the legal requirement for a signature. But where ESIGN applies to "any transaction in or affecting interstate commerce," UETA only applies to transactions arising out of business, commercial, and governmental matters. UETA also carves out exceptions and does not apply to birth certificates, wedding certificates, death certificates, wills, codicils, and testamentary trusts.

Illinois, New York, and Washington

Illinois, New York, and Washington have all adopted laws other than UETA.

Illinois adopted the Electronic Commerce Security Act in 1998. The most notable difference in Illinois law is that it favors some types of electronic signatures to others. Notably, it denotes "secure electronic signatures" as the most secure type of e-signature. By Illinois's standard, an electronic signature is secure if it 1) is created in a commercially reasonable manner, 2) is applied by all parties in a

trustworthy manner that can be verified, 3) can be reasonably and in good faith relied upon by all parties, and 4) is agreed to be secure by all parties.

New York has the Electronic Signatures and Records Act (ESRA) from 2000 which established the legal equivalence of electronic and handwritten signatures. ESRA also provides for an “electronic facilitator” whose role is to publish a best practices guide for e-signatures to be in compliance with ESRA.

Washington has the Washington Electronic Authentication Act (WEAA) enacted in 1997. This act ensures that electronic signatures are not refused legal recognition and delves into the verification process so that users may know that a signed document has not been altered. WEAA’s verification process works by establishing standards for how “certificate authorities” can issues credentials to individuals. These credentials then allow the individual to create a digital signature which comes with the assurance that the digitally signed documents are attributable to the signer and have not been altered. This verification process is not widely used in commercial agreements and has been effectively relegated to use with state agencies.

Compliance

While e-signature law is meant to promote the convenience of electronic communication, there are some important standards to keep in mind. To be compliant with e-signature laws, standard practice suggests that e-signature workflows must:

- validate identity
- demonstrate intent to sign
- demonstrate consent to do business electronically
- provide opt-out options
- distribute signed copies to the participants
- retain records
- demonstrate proof of signing

Each of these standards will be briefly discussed below. As with all contracts, the identity of the signer must be established for the contract to be valid. The identity of the signer is an evidentiary issue that will come up in court if the contract is disputed. Fortunately, identity can be easier to prove with an e-signature than with a paper-based signature. Identity can be established through the use of an email address, IP address, corporate ID, password, pin or other similar elements associated with the signer.

Filevine's Vinesign offering uses email addresses and phone numbers to verify the identity of the signer and collects the signer's IP address when the document is signed. Additionally, in some jurisdictions, Vinesign offers gesture verification that allows the signer to upload a picture of themselves as verification. These same identity verification resources are not available when relying on a paper-based signatures.

Demonstrating intent to sign is also mandatory in determining the validity of a contract and is often demonstrated by the style of signature or method of contracting. Different styles of obtaining an e-signature demonstrate intent with varying levels of credibility in the courts. One of the most credible forms of e-signature are free-form signatures on a touch screen or a text version of the signer's name. Vinesign offers the option for free-form signatures either through using a finger on a touch screen or a mouse on a desktop.

Another form of agreement generally upheld by courts is a click-wrap agreement that requires the click of a button or checkbox indicating agreement to a set of terms before the user can proceed with a transaction. Browse- wrap agreements that require some action of the user, sometimes as simple as continuing to visit the website, to demonstrate acceptance of the terms are also often upheld by courts but less frequently than the other methods mentioned. In all of these methods, enforceability hinges on whether the user had actual and constructive notice of the applicable terms and demonstrated the intent to sign them. This standard should be given priority when determining which method of contracting to use.

Different styles of obtaining an e-signature demonstrate intent with varying levels of credibility in the courts.

The other elements of standard practice are relatively simple. Consent to do business electronically can be demonstrated with a standard "click to accept" consent clause. The opt-out option should involve clear instructions on how to sign the agreement manually. Importantly, ESIGN permits businesses to make disclosures electronically as long as the consumer is provided with notice of the consumer's ability to receive the information on paper and information about the hardware/software needed to access the information electronically. After the documents are signed or agreed to, all signers should receive a copy of the fully executed agreement. Vinesign offers the signer the option to download the document after signing. Additionally, the owner of the document gets a signed copy accessible through Vinesign. Moreover, where

Vinesign is integrated with Filevine, the owner also receives a copy of the signed document in their Filevine project.

ESIGN also requires that e-signed documents be reproduced as needed. Vinesign meets this standard by storing signed documents that are only deleted at the owner's discretion. Finally, proof of signing can be demonstrated through use of an audit trail and tamper-evident digital certificate embedded in the completed document. Each document signed through Vinesign is given a unique code used to certify the signature and avoid tampering. The document is also flattened to disallow editing after the signature.

As highlighted above, the use of e-signatures can be simple and convenient as long as standard practices are maintained.

filevine.com