SignNow

Legality of Electronic Signatures

White Paper

The validity and enforceability of electronic signatures has been well established in the United States for over fifteen years. In 2000, Congress passed the Electronic Signatures in Global and National Commerce Act (ESIGN), establishing that e-signatures shall have the legal equivalence of wet signatures. Additionally, all 50 states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted state laws validating e-signatures, with all but three adopting the Uniform Electronic Transactions Act (UETA). Illinois, New York and Washington, have not adopted the UETA, but have similar statutes validating electronic transactions.

GENERAL RULE OF VALIDITY

UETA and ESIGN both state: "a record or signature may not be denied legal effect or enforceability solely because it is in electronic form." These statutes establish the general rule that electronic signatures are valid and enforceable, provided certain requirements are established.

WHAT'S REQUIRED

Consent
All parties to an agreement or transaction must agree to conduct the transaction using electronic means. Consent to conduct transactions using electronic means will be determined by the parties' conduct and may be either express or implied. The action of electronically signing a document will generally satisfy this requirement.

Intent
In order to be valid, it must be clear that the signer intended the designated e-signature act or process to constitute an electronic signature. Intent to sign may be established when a person affirmatively attaches a digital signature to the document using a touch screen or click of a mouse and clicking a "submit" or "done" link.

Association
An e-signature must be connected to the document that is being signed. When using a digital signature, the signature is electronically attached to the electronic document at the time it is signed and saved as a PDF document.

Attribution
The e-signature must be attributable to the person who is signing. The attribution of an eSignature to a person will be determined based on the context and circumstances under which the document is signed. This can be done by a variety of means, including

documenting the communications and actions of the parties, and recording metadata such as date/time stamps and IP addresses.

Record Retention

An electronically signed document must be in a form that is capable of being retained and accurately reproduced for later reference by all parties or persons who are entitled to a copy of the document or record.

ADMISSIBILITY OF ELECTRONIC RECORDS

The validity and admissibility of e-signatures is well established and rarely challenged. In the few cases where an e-signature has been challenged, the Courts tend to focus primarily on whether there was an intent to sign and/or the attribution of the signature to the person at issue. Establishing intent and attribution generally involves an examination of the processes by which the signature was captured, secured, and stored. Therefore, it is important to maintain a detailed audit trail that logs the actions taken by the parties electronically signing documents. This detailed audit trail will also help ensure that the electronic document can be authenticated and admitted under the applicable rules of evidence.

SIGNNOW LEGALLY BINDING SIGNATURES TRUSTED BY USERS

SignNow complies with ESIGN and provides additional security and authentication options above and beyond what is legally required by ESIGN.

- Unique Signatures for Each User: When a document is sent to a user for signature, SignNow invites the user to create a unique signature that is attributable to that user and saved for future use. Signature options include typing in a name and selecting a SignNow created e-signature, hand written digital ink signature using a finger or mouse, or uploading an e-signature. Once selected, the user clicks a button indicating their intent to make the designated e-signature a legally valid electronic signature.

- Signer Authentication: Information tracked and available to identify signers includes email address they had access to when signing the document, IP address, and exact time of document access. SignNow also offers the option to add two-factor authentication to any document sent for signature. This allows the document custodian to set an individual password for some or all of invited signers and then transmit that password to each signer independent of SignNow.

- Retention in the Cloud: Documents are stored on Barracuda's secure cloud platform. Any registered user who signed or otherwise took action in connection with a document will be able to view or download a copy of the final PDF e-signed document upon creating a SignNow account.

- Detailed Audit Log: SignNow also creates and maintains an audit log, which shows the entire history of a document, including uploading, adding elements, viewing, signing, and who took each of these actions. The audit log tracks metadata associated with each of these actions, including information about the authenticated user, the date, the IP address, and which platform 07/13/2015 BARRACUDA NETWORKS CONFIDENTIAL AND PROPRIETARY PAGE 3 OF 3 LEGALITY OF ESIGNATURES WHITE PAPER was used (web, iOS, Android). The audit log is viewable directly with the SignNow app or can be appended to the PDF document through the Download with History feature.

- Security: All documents and data are encrypted while in transit using our state of the art encryption technology.