Exploring Admissibility of Electronic Records and Electronic Signatures

Jim Damian, MSW
Founder / CEO of Stria, LLC
July 2018

Stria regularly advises clients that electronic records are generally accepted as legally admissible. This stance assumes that the electronic records in question were produced in accordance with a high-quality process (methodology) that is well documented and executed by qualified personnel. Further, Stria advises clients that several different electronic signature formats are legally admissible under most circumstances. This paper explores and references laws surrounding electronic records and electronic signatures.

Electronic Records

Courts have upheld that electronic records created through imaging or scanning are just as legally binding as paper documents. However, legal admissibility of electronic items requires that a high-quality and well documented business process be used to create the electronic records.

In the United States, two uniform laws clearly establish the basis for admitting

electronic records as evidence. The first key law governing the admissibility of electronic records is the Uniform Photographic Copies of Business and Public Records as Evidence Act (28 U.S. Code § 1732). This law states that "If any business, institution, member of a profession or calling, or any department or agency of government, in the regular course of business or activity has kept or recorded any memorandum, writing, entry, print, representation or combination thereof, of any act, transaction, occurrence, or event, and in the regular course of business has caused any or all of the same to be recorded, copied, or reproduced by any photographic, photostatic, microfilm, micro-card, miniature photographic, or other process which accurately reproduces or forms a durable medium for so reproducing the original, the original may be destroyed in the regular course of business unless its preservation is required by law."

A logical and common interpretation of this law is that physical paper (or "source") documents can be destroyed after reproduction or scanning, since the new digital copy has become the legally binding and admissible document.

The Federal Rules of Evidence also provide clear guidance on the admissibility of electronic records. Rule 1003- Admissibility of Duplicates states that: "A duplicate is admissible to the same extent as the original unless a genuine question is raised about the original's authenticity or the circumstances make it unfair to admit the duplicate."

Rule 1003 has been adopted by the United States federal courts along with most state courts. Digital records created by a responsible service provider using a rigorous and well documented process would likely be admissible. Digital records created by unscrupulous providers or created without a well-documented process are more likely to be challenged as admissible and/or legally binding.

Both of the aforementioned laws admit duplicate (or scanned) records into evidence if they accurately reproduce the original because document imaging technology is a duplication technology similar to photocopies, microfilm and facsimile.

The most widely□used reproduction techniques, including photocopy, microfilm, facsimile and document imaging all exhibit the same characteristics.

Electronic Signatures

Electronic signatures are acceptable under the Uniform Electronic Transactions Act (UETA). UETA specifies, in general

(a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

(b) A contract may not be denied legal effect or enforceability solely

because an electronic record was used in its formation.

(c) If a law requires a record to be in writing, an electronic record satisfies the law.

(d) If a law requires a signature, an electronic signature satisfies the law.

UETA defines "electronic signature" as follows:

(8) "Electronic signature" means 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.

This means that when an employee reads the content, selects a check box, types in their name and clicks on the "save" button, they have electronically signed the document.

The United States Electronic Signatures in Global and National Commerce (ESIGN) Act also governs admissibility of electronic signatures. This act calls four major requirements for an electronic signature to be recognized as valid under U.S. law. Those requirements are:

1. Intent to sign – Electronic signatures, like traditional wet ink signatures, are valid only if each party intended to sign.

2. Consent to do business electronically – The parties to the transaction must consent to do business electronically. Establishing that a business consented can be done by analyzing the circumstances of the interaction, but consumers require special considerations.

3. Association of signature with the record – In order to qualify as an electronic signature under the ESIGN Act and UETA, the system used to capture the transaction must keep an associated record that reflects the process by which the signature was created or generate a textual or graphic statement (which is added to the signed record) proving that it was executed with an electronic signature.

4. Record retention – U.S. laws on eSignatures and electronic transactions require that electronic signature records be capable of retention and accurate reproduction for reference by all parties or persons entitled to retain the contract or record.

Legal validity, court admissibility, and enforceability are not the same thing. Each concept has a distinct definition, set of requirements, and, most importantly, contribution to the outcome of a legal dispute.

While the ESIGN Act states that signatures should not be denied legal validity solely because they are electronic, a judge's willingness to accept that contract could depend on how the electronic document was signed.

Certain criteria must be met in order for an e-signature to be admissible in court. Any entity who hopes to present an electronically signed contract in front of a judge needs to be able to prove the

intent of the signatory and the security of the signed document. If the document could have been tampered with or altered in any way after it was signed, there is a likelihood that a judge will refuse to allow it to be admitted in court. Specifically, an e-signed document may be legally valid but ruled inadmissible in court due to weaknesses in security, audit logs, or authentication. Tt is critical that businesses select an e-signature solution that is highly reputable and meets the highest standards of technical integrity.

Finally, the enforceability of a contract depends not only on its validity and admissibility, but also the contents of the agreement itself. In a dispute, a judge may examine an agreement to evaluate for clear and consistent terms, proper consideration undue influence, and intent.

Conclusion

Electronic records and electronic signatures are as legal as they are efficient. However, selecting the right partner to design, document and deploy the systems and methods is very important. Organizations should also have internal counsel provide a legal review in conjunction with new electronic record or electronic signature processes, procedures or platforms.

Contact Information

Jim Damian, MSW
Founder / CEO
Stria, LLC
www.Stria.com
877.839.8952