

Onboarding Fact Sheet: Electronic Signatures

Electronic Signatures Regulation

The adoption of the Uniform Electronic Transactions Act (UETA) in most states and the passage of Electronic Signatures in Global and National Commerce Act (ESIGN) at the federal level in 2000 solidified the legal landscape for use of electronic records and electronic signatures in commerce.

Rule of General Validity

Both ESIGN and UETA establish that electronic records and signatures carry the same weight and legal effect as traditional paper documents and handwritten signatures, stating:

A document or signature cannot be denied legal effect or enforceability solely because it is in electronic form.

Intent to Sign

The electronic signature laws retain the rule that a signature is only valid if the signer intends to sign.

Signature Associated with the Record

In order to qualify as an electronic signature under ESIGN and UETA, the system that is used to capture the electronic transaction must either

1. keep an associated record reflecting the process by which the signature was created or
2. make a textual or graphic statement that is added to the signed record, reflecting the fact that it was executed with an electronic signature.

Consent to Do Business Electronically

Because onboarding is a business transaction, the nature of the parties' consent to do business electronically can be established explicitly or by implication based on the parties' interactions.

However, in some cases, during the onboarding process, there can be consumer related transactions between a financial institution and a consumer that occur primarily for personal, family or household purposes such as a loan to the onboarded individual.

Consumers interacting with financial institutions receive special protection under ESIGN and some state UETA enactments. Electronic records may be used to deliver Required Information to consumers only if the consumer:

1. receives certain disclosures (UETA Consumer Consent Disclosures);
2. has affirmatively consented to use electronic records for the transaction; and
3. has not withdrawn such consent.

ClearCompany therefore provides a Consumer Disclosure link on all onboarding packets that can be referred to in the documentation and affirmatively accepted before signing should the forms contain consumerrelated services with a financial institution that require consumer consent.

Record Retention

UETA provides that legal effect, enforceability or validity requires that electronic signature records be:

1. capable of being retained; and
2. capable of being accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record.

The Legality of Electronic Signatures

Contracts signed using enterprise-level electronic signature processes like ClearCompany are completely secure and deliver a rigorous audit trail of who signed and when. This court admissible audit trail includes the core elements required to successfully enforce and defend a contract.

ESIGN – Best Practices

Compliance with the e-signature laws is a very basic step in selecting a system for electronic signature transactions. Like their paper counterparts, electronically signed documents can become the subject of a dispute.

In the event of a dispute regarding an electronically executed contract, merely complying with ESIGN is not enough. The signature process must provide enough proof to uphold the transaction.

Our comprehensive approach includes important security features such as:

- Secure encryption so documents can be read and signed only by designated users
- Signature lines in most forms so users can 'initial' and 'sign' specific areas of a document
- User Authentication leveraging email, and an access code

Intent to Sign

A key convention in the paper world, precise signature placement is important criteria in establishing the signer's intent. Similar considerations should be made when adopting an electronic signature process.

Record Retention

Few organizations find the requirements for record retention under UETA and ESIGN strict enough in comparison to their standards for mitigating risk. Most notably, the storage systems associated with any electronic

signature system must be rigorously secure from a physical and technological standpoint.

Admissibility into Evidence

The Federal Rules of Evidence and the Uniform Rules of Evidence generally allow for electronic records and their reproductions to be admissible into evidence. This applies to electronic signatures stored in a computer or server, so that any printout or output readable by sight, shown to reflect the data accurately, is considered an original. In the case of an electronic signature, then, it is important to demonstrate to the satisfaction of the courts that:

1. the appropriate level and amount of information surrounding the signing process was retained, and
2. the system used to retain the information is itself reliable.