E-signatures: When They’re Legal and Best Practices for Implementation

Introduction

Companies that have adopted (or plan to adopt) e-signature solutions should consider the legal and risk management factors associated with e-signatures. The following is an overview of these factors, including when e-signatures legally bind a party to perform under a contract and how companies can mitigate risk when adopting e-signature solutions.

Legal Overview of E-Signatures

There are two statutes that speak to e-signature legality in most of the United States. The first is the federal Electronic Signatures in Global and National Commerce Act (ESIGN), which went into effect on October 1, 2000. The second is the Uniform Electronic Transactions Act (UETA), which was originally drafted in 1999 and has been adopted in substantially the same form by every state except for New York (and Puerto Rico). Although New York has not adopted the UETA, New York’s Electronic Signatures and Records Act (NYESRA) was drafted to be consistent with the ESIGN. Similarly, Puerto Rico enacted the Electronic Signatures Act. Contact your ArentFox Schiff connection for specific guidance in these jurisdictions.

A few key concepts underlie e-signature laws in the US.
1. ESIGN provides that “a signature, contract, or other record related to any transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form.” In practical terms, this means that, assuming there are no other legal issues, e-signatures have the same binding legal effect as wet ink or in person signatures.

2. No specific technology is required for an e-signature to be legally binding. For example, courts have upheld “clickwrap” agreements that require only an affirmative “click” from the user (as long as the user has reasonable notice of the contract terms before clicking through and the click-through reasonably manifests their assent).

3. ESIGN expressly preempts non-conforming state laws. This means that in the event of a conflict between a state statute concerning e-signatures and ESIGN, the relevant provisions of ESIGN will govern, rather than the inconsistent state law provisions.

While both ESIGN and UETA broadly define “transaction” to include almost all transactions, there are certain contracts that are excluded from ESIGN’s provisions. ESIGN’s permissive provisions do not apply to “wills, codicils, or testamentary trusts,” family law matters, or certain provisions of the Uniform Commercial Code. ESIGN also excludes signatures to official court documents and certain consumer agreements (e.g., utility services or product recalls).

Changes in technology have led several states to update their versions of the UETA. For example, several states in recent years have updated their versions of the UETA to keep pace with the rapid development of blockchain technology. In general, these updates recognize that a contract generated using blockchain technology must be given the same effect as other e-signatures covered by UETA. States have also enacted laws providing that courts may not invalidate a contract because it contains a “smart contract” term.

Although the rising prevalence of e-signatures has implications for practically every industry, it is especially prevalent in the commercial real estate industry. The provisions of ESIGN and UETA recognize electronic notarization of documents. Several states have adopted laws authorizing remote online notarization (RON) of real estate transaction documents. The specific provisions of RON laws vary from state to state. In general, each state’s RON law (i) allows notarization via audio or video communication (even if the signer is outside of the notary’s authorized state); (ii) requires that the notary authenticate the person signing; and (iii) requires recording of the audio or video communication through which the notarization takes place.

When disputing the validity of an e-signature in court, e-signatures are subject to the same evidentiary rules as traditional, wet ink signatures. In other words, in order to successfully enforce an agreement signed by e-signature, companies using e-signature solutions must ensure that they have standardized business processes in place.

Potential Risks with E-Signatures

As with any business process, there are some practical risk management issues that companies should address for e-signature practices. These risks exist with wet ink signatures, but, because of the speed and ease of executing a contract electronically, the risks may increase with convenience.

Compliance Risks
There are compliance risks posed by the use of e-signatures. Companies that take advantage of this process should confirm that their business is not subject to regulations that would restrict the use of e-signatures.

For example, under ESIGN, if a federal statute or regulation calls for notice to be provided to a consumer in writing, a company must meet several notice requirements before it can provide consumers with written notices electronically. Recently, four Senators introduced a bill to modernize ESIGN by (i) removing the requirement that a consumer “reasonably demonstrates” his or her ability to access information in electronic form before receiving them electronically, and (ii) requiring that an entity only needs to provide a statement informing the consumer that the hardware and software required to access information has changed. Several states also impose notice requirements, among other regulations, on automatically renewing consumer contracts, which many consumers may opt to sign electronically.

In addition, companies operating in industries regulated by the FDA must take care to comply with the requirements in 21 CFR Part 11 concerning electronic records and e-signatures.

Failing to observe compliance requirements associated with e-signatures may excuse counterparties from their obligations under an agreement with the company and subject the company to regulatory sanctions. Properly designed e-signature processes will allow companies to exploit the convenience and ease of e-signature solutions while remaining compliant with applicable regulatory standards.

**Authentication and Repudiation Risk**

Authentication issues may also arise when companies use e-signature solutions for contracts. While laws may address the issue of whether an e-signature qualifies as a signature, they do not touch on whether an e-signature is a particular party’s signature. An e-signature may be forged just as easily (or more easily) as a wet-ink signature. If there is a dispute over the authenticity of an e-signature, each side will have to prove “who signed what.” Companies that do not take steps to authenticate the attribution of e-signatures may find it difficult to enforce an agreement in the future. This can cause damage to a business’ reputation, internal controls, and bottom line.

In addition, companies assume the risk that a party will repudiate the contents of an electronically signed document by claiming the document’s contents changed after the party affixed its e-signature. These disputes will turn on issues of fact, specifically, when and whether a document was modified compared to when it was signed. Frequently, a contract will allow one party to unilaterally update its terms without notice. Parties should make sure that their contract is clear as to when and how one party can unilaterally change the terms of the contract, particularly when executing contracts with e-signature solutions.

Practically speaking, these are not novel issues – companies also assume authentication and repudiation risks when using wet-ink signatures, particularly when using “breakaway” wet-ink signature pages. Fortunately, most e-signature solutions provide security features that allow companies to mitigate these risks.

**Security Features in E-Signature Solutions**

Companies can benefit from significant security improvements to their contracting processes by adopting e-signature solutions:
Identity Verification. Most basic versions of e-signature solutions require signers to verify their identity through (i) their email; or (ii) some form of two-factor authentication. Companies that desire a higher level of security for certain agreements may benefit from using digital signature technology, which we discuss in further detail below.

Document Security. One of the primary ways that e-signature solutions maintain document security is with an audit trail embedded in the document. The audit trail is a digital log with a timestamped archive of signatures detailing when each party opened, viewed, and signed an agreement. In some cases, additional details can be collected, such as the IP address or geolocation associated with the signature.

Companies should review the security standards provided by the e-signature providers at both the signature and document level. E-signature providers should provide strong data encryption in transit and at rest. Companies can further explore security options available through various e-signature providers, such as whether their e-signature solutions use hash functions to both verify and secure each record of the document and the audit trail. These generate unique identifiers (i.e., hashes) for each record that determine whether a document was altered before or after the signature.

Digital Signatures

Digital signature solutions use Public Key Infrastructure (PKI) protocol to generate two numbers, or “keys,” associated with a signature. One key is public, and one key is private. The private key is used to sign and encrypt the document. When the signer sends the agreement to another party, it will send a copy of its public key. If the keys do not match, the recipient cannot decrypt the signature. In other words, only a signer’s public key will unlock the document protected by the signer’s private key. Digital signatures help make sure each signatory is the right person signing the right document.

Conclusion

By tailoring e-signature processes to account for legal and other risks, companies can maximize the benefits offered by e-signature solutions. Companies should also review their e-signature processes to ensure that they incorporate the most recent advances in security and authentication technology.

© 2023 ArentFox Schiff LLP

National Law Review, Volume XII, Number 136

Source URL: https://www.natlawreview.com/article/e-signatures-when-they-re-legal-and-best-practices-implementation