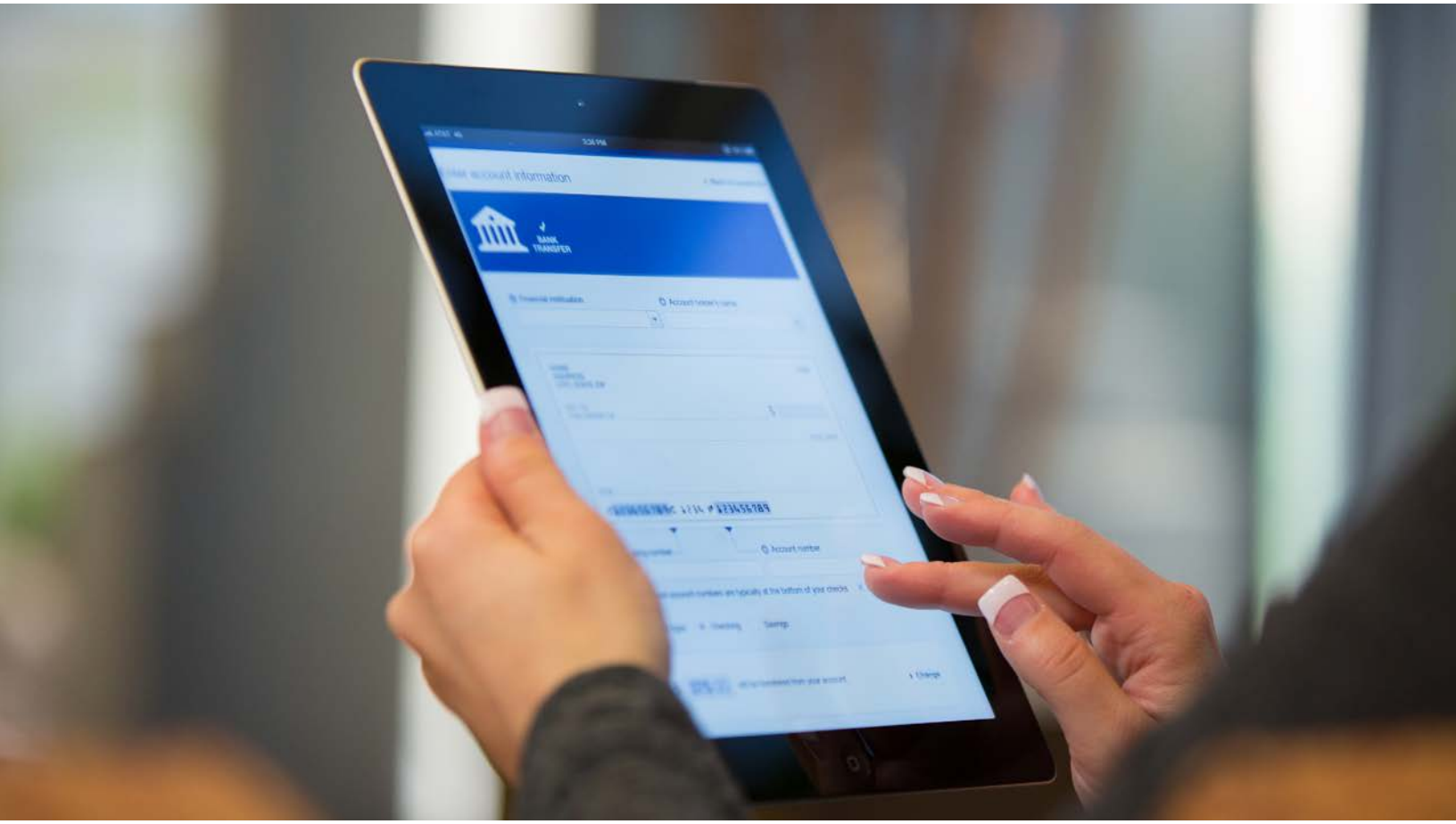
ESIGN Act: A Well-Established Law Enabling Business Transformation Today



ESIGN Act: A Well-Established Law Enabling Business Transformation Today

A guide to electronic signatures in the United States for corporate counsels and compliance officers

Table of contents

On June 30, 2000, President Bill Clinton signed the *Electronic Signatures* in Global and National Commerce Act (ESIGN Act) into law without a pen. Instead, he used an *electronic signature*. This ground-breaking law addresses *e-signatures* as well as electronic records, both of which are commonly used in commerce today. An *e-signature* was granted the same status as a written signature under the terms of this legislation; however, it is important to note that simply placing a symbol on a document does not, in and of itself, create an enforceable contract. Those who are concerned about the question of legality must be well informed about the various requirements associated with the use of e-signatures. For most, the first and foremost question may be, "Are e-signatures legal?"

The simple answer is, yes, e-signatures are legal. This paper discusses several factors relating to the legality of e-signatures in various applications and among different industries, with their associated regulatory environments. It also explores the benefits of adopting a digital document solution that enables real-time signatures. When used along with sound and consistent best practices, the optimal solution can not only create an enforceable contract, but also improve document creation, storage, retrieval, and audit trails.

E-signatures are fast becoming an integral part of our business landscape. Leading companies today, even in the most conservative and regulated industries such as financial services and healthcare, are rapidly adopting e-signatures to accelerate key business processes. For example, a leading healthcare company estimates that by using *Adobe Sign*, they decreased transaction costs from US$16 to US$1.50. These cost-saving benefits, in addition to the improved ease and efficiency of transacting business, will undoubtedly fuel the continued growth of e-signatures.

ESIGN Act makes e-signatures legal

The ESIGN Act of 2000 addresses electronic signatures as well as electronic records, both of which are commonly used in commerce today. Due to federal preemption, the ESIGN Act allows electronic signatures in all 50 states when federal law applies. Where federal law does not apply, every state has an electronic signature law, most following the Uniform Electronic Transactions Act (UETA).

The ESIGN Act:

- Satisfies most statutes, that require handwritten signatures on documents
- Allows the contract to be used as evidence in a court of law as long as surrounding processes are well designed and implemented and the usual elements of a contract exist
- Prevents denial of legal effect, validity or enforceability of an electronically signed document solely because it is in electronic form

According to the ESIGN Act, an e-signature is defined as "an electronic sound, symbol, 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 and be legally bound." The key takeaway for purposes of contract enforcement is that the electronic sound, symbol, or process must be both associated with a contract or other document and adopted by the signatory, by some act, with the intent to be bound.

E-signature solution selection is key to meeting industry requirements

The broad nature of the ESIGN Act created an opportunity for regulators in various industries to make specific rules pertaining to the use of e-signatures. The ESIGN Act provides that both federal and regulatory agencies have the authority to interpret and apply the law in the context of their industries. Understanding the implications of e-signature use in a specific industry depends upon consideration of the reason the document was created. If the document is being generated for business, consumer, or commercial transactions, the ESIGN Act generally supersedes any regulatory agency's preexisting requirement that a record be kept on paper. However, if it is being created principally for governmental requirements not related to commercial transactions, the ESIGN Act may not apply.

The use of electronic signatures may satisfy the requisite regulatory compliance in your industry by providing the authentication, authorization, accountability, audit, and security needed to follow your industry's particular laws. The following table offers a summary of several major industry regulations coupled with the important features of a robust e-signature solution relating to those regulations.

Industry regulation	Overview of regulation	What to look for in an e-signature solution
Sarbanes-Oxley Act (SOX)	SOX requires that publicly held corporations establish verifiable security controls to protect against disclosure of confidential data and carefully track personnel data to detect fraud-related tampering.	Solution should include robust and comprehensive security safeguards such as infrastructure security and data security, including application-level encryption using Secure Sockets Layer (SSL) and 256-bit Advanced Encryption Standard (AES) encryption, to safeguard the confidential information in an electronic document.
Gramm-Leach-Bliley Act (GLBA)	GLBA is intended to protect consumers' privacy and provide security for consumer personal information, requiring notification and opt-out procedures and limiting the reuse or marketing of consumer personal information.	The technology must provide for the safety of any personal information captured, clearly explain notification and opt-out procedures to the consumer, and strictly limit reuse or marketing of a consumer's personal information.
Dodd-Frank Act (DFA)	DFA created the Consumer Financial Protection Bureau (CFPB), a council designed to oversee financial institutions and reform securitization. E-signatures comply provided that they adhere to the consent requirements of the federal ESIGN Act.	The solution must provide for active consent of the signatory prior to applying the e-signature to the document.
Federal Deposit Insurance Corporation (FDIC)	FDIC regulations relating to electronic filings and signatures require a signature to appear in "typed form" and require an electronic copy of the physical signature for anything electronically signed.	The solution should provide a "typed form" appearance as well as maintain an electronic copy of the physical signature for any document executed with an electronic signature.
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	HIPAA places stringent requirements on healthcare providers (also called "Covered Entities") to protect sensitive health information.	Companies must work only with HIPAA-compliant service providers and have a Business Associate Agreement (BAA) in place with those providers. The solution must support HIPAA's stringent privacy and security requirements to protect sensitive data, and the company's BAA must meet all HIPAA requirements.
Internal Revenue Service (IRS)	Currently, the use of e-signatures on IRS forms is approved on an ad hoc basis. According to Announcement 2013-8, the IRS requires that signatures meet five core requirements that align precisely with the ESIGN Act.	The solution must show that the electronic form of signature that is adopted by the signatory with the intent to be bound is attached to the record being signed, authenticated, and properly preserved and stored.
McCarran-Ferguson Act (Public Law 15)	The ESIGN Act expressly states that it applies to the business of insurance to comply with the McCarran-Ferguson Act. The ESIGN Act also includes a specific provision that relieves insurance agents and brokers from liability under certain conditions.	The solution needs to comply with the ESIGN Act such that insurance agents can meet the requirement that an action be legally attributable to a person intending to be bound. Simple compliance with the Uniform Electronic Transactions Act (UETA) does not achieve this industry best practice.

Court rulings focus on intent to be bound and processes used

The courts are catching up to the reality of e-signature technology in the modern business climate. The main issues that result in legal conflicts do not tend to arise around the technicalities associated with an e-signature but rather with the various elements of contract formation, that is, the facts surrounding creation of the contract. So, processes relating to capture, security, storage, and retention are important.

For example, the New York Supreme Court addressed whether precise adherence to the definition of an e-signature is required to create a valid agreement. In *Forcelli v Gelco* (2013) 109 A.D.3d 244, a case involving settlement negotiations via email, the court concluded that a farewell statement at the end of the email was a signed and "subscribed" signature even though it did not technically constitute an e-signature according to statute.

Evidence of a clear intent to be bound is important. Courts generally require evidence of an awareness of the terms of the contract and an act that exhibits assent or intent to be bound prior to signing a document or using a service, like clicking an "I agree" button. However, some courts do look at the circumstances surrounding the transaction for other indications of assent and have held that a contract is enforceable even without such an overt indication.

Additional important topics covered by the courts are evidentiary issues such as preservation and admissibility of electronically stored information (ESI). At the most basic level, such information must be properly preserved and then admitted. The leading case on the admissibility of ESI, *Lorraine v Markel AM. Inc. Co.* (2007) 241 F.R.D. 534, addressed a failure to comply with the rules of evidence surrounding the submission of extrinsic information to resolve an ambiguity in an arbitration contract. The court analyzed the admissibility and addressed the importance of ensuring that a document is authentic or that it is what it claims to be, that it is an accurate duplicate of the original to satisfy the original writing rule, and that business records are kept in the normal course of business to overcome the hearsay exclusionary rule.

The bottom line is that your documents are only as good as the process you used to obtain them. In the event of a legal challenge to your document, your electronically stored information must have been properly obtained, preserved, produced, and ultimately admitted into evidence. The success of this effort may in large part depend upon whether you diligently followed your own process. And if you don't provide the appropriate level of assurances, the document could be deemed inadmissible.

Recommended process and best practices for adopting e-signatures

When adopting e-signatures, your process should involve the following:

- **Authentication**—Authenticate the signatory's identity.
- **Consent**—Account for consent.
- **Intent to be bound**—Establish intent to be bound.
- **Attribution**—Establish attribution to a particular individual and/or a representative of a company.
- **Security**—Provide a binding of the signature to the document and proof of nonalterability after the signature has been affixed to the document.
- **Record retention**—Offer secure storage and access processes.

The process of creating a valid e-signature requires that the signer be identified and authenticated at the time of the signature. To meet the requirements of state evidence laws on authentication and FRE 901(a), the law generally requires that a proponent of a document produce sufficient evidence to support a finding that the item is what he or she claims it to be, and that the signing process be sufficiently described to show that it produces an accurate result.

The following best practices can help guide you in developing your document creation, storage, and retention processes to ensure admissibility of a document:

- **Create an audit trail**—Identify your signatory; which document was signed; and when the document was signed, including date, time, and sequencing of events. Ensure that any changes to records do not obscure previous entries. This audit trail also includes ensuring that the signatory affirmatively consented to the e-signature process and has not withdrawn such consent.
- **Secure the audit trail**—Render the *e-signed* document unalterable within a secure "electronic vault." Securing the audit trail also describes the internal process ascribed to storing electronic records. Electronic records must be capable of being retained and accurately reproduced for later reference.
- **Create and maintain a retrieval process**—Appoint a credible custodian of records to manage the process. This person should also be able to testify to the secure steps taken by all company representatives in the e-signature and e-storage process, rendering documents accurate and readily retrievable.

E-signatures accelerate key business processes

E-signatures can deliver quick and impressive ROI, while enabling significant improvements in security and compliance. Some common use cases include:

- **Accelerate sales documents**—Decrease the time to revenue and increase the deal closure rate by automating the creation of electronic sales documents and contracts and enabling customers to sign electronically. Integration of the e-signature process can be part of a CRM deployment, such as with Salesforce, Workday, Microsoft Dynamics CRM, SAP, or NetSuite, so the entire process remains electronic. See Adobe Sign case studies: Groupon, Ricoh UK, NetApp.
- **Simplify employee onboarding and policy acknowledgements**—Speed up HR processes such as offer letters, new hire documents, and employee policy acknowledgements by eliminating printing, faxing, and overnight mailing. The e-signature process can be standalone or embedded into a human capital management system, such as Workday, Successfactors, or Taleo. See Adobe Sign case studies: Telefonica, Foursquare.
- **Streamline legal and procurement operations**—Automate the process for nondisclosure agreements, vendor contracts, and confidential business-to-business agreements. Standalone or integrated into a contract management system such as Ariba Contract Management, SAP CLM, Oracle, or NetSuite, e-signatures can accelerate the execution of contracts by as much as five times or more. See Adobe Sign case studies: Leasedrive, TiVo, Kantar IT Partnership.

"We can complete contracts in minutes and meet deadlines that would have been impossible without leveraging this type of technology."

Connie Brenton, director of operations and chief of staff, legal department, NetApp

Adobe Sign is the trusted solution used by many of the Fortune 1000

Adobe Sign is an Adobe Document Cloud solution that speeds business, integrates with existing systems, and reduces signature cycle times from days to minutes—all from the trusted leader in secure digital documents for over 20 years. Global companies choose Adobe Sign to drive business faster, enabling real-time signatures and approvals—easily, securely, on any device.

With careful application design, rigorous security practices, and continued monitoring of the global landscape via legal teams across 30 offices worldwide, Adobe enables companies to maintain compliance with federal and industry regulations so they can have peace of mind. Following is a summary of how Adobe Sign enables compliance with legal standards and best practices.

- **ESIGN Act compliance**—In the United States, Adobe warrants that Adobe Sign is fully compliant with the ESIGN Act of 2000. In addition, it complies with the European Union regulation on electronic identification and trust services (eIDAS), Australia's Electronic Transactions Act, Canada's Uniform Electronic Commerce Act (UECA), the Electronic Communications Act 2000 (c. 7) in the United Kingdom and more.

- **Robust security at every level**—Adobe uses the same technologies and security engineering processes relied upon by financial institutions and governments around the world. Each release of Adobe Sign code, along with the infrastructure that supports them, is developed with the Adobe Secure Product Lifecycle (SPLC) framework. The SPLC framework is a rigorous set of best practices, processes, and tools used throughout product development, resulting in more secure code that safeguards confidential information. Infrastructure security is achieved through a multilayered approach that includes physical security, firewall security, real-time logging and monitoring, intrusion detection, and data security. Adobe Sign is supported by state-of-the-art, geo-dispersed data centers to provide data redundancy and availability. SSL and AES encryption safeguards the integrity of documents, in motion and at rest. Authorization to access different data sets is based on user roles within the application. The user must be a participant in the contract (such as the document sender or signer) to view or modify the contract.
- **Compliance with SOC 2 Types 1 and 2, ISO 27001, GLBA, HIPAA, PCI DSS, and the US-EU Safe Harbor Framework**—Adobe Sign generally meets or exceeds the strict standards arising from the varied and complex regulatory landscape. Contact your Adobe representative to learn more about how Adobe Sign is designed to meet your specific regulatory compliance needs.
- **Best-in-class e-signature support for strong legal protection**—Adobe Sign offers multiple authentication methods including multi-factor authentication before opening the document to sign, as well as support for signing with certificate-based digital IDs. Signatories can be required to provide their consent to use Adobe Sign before their electronic signatures can be applied to the document. Every document signed with Adobe Sign automatically generates an audit trail that tracks every step in the signature process—from initial document preparation through signing and archiving. This comprehensive audit trail is encrypted, digitally sealed, tamper evident, and stored securely so that it can be used in court to help prove who signed a document and when they signed it.

"We initially looked at Adobe Sign just for legal contracts, but we've discovered that it has so many more applications than we expected. Adobe Sign is helping us streamline internal and external operations across the company, making it one of the most value-added products we've ever seen at TiVo."

Larry Denny,
vice president and
associate general
counsel, TiVo

Without a fully digital business, the greatest risk is being left behind

Digital and mobile technologies have become the standard for business communications today. Gartner predicted that mobile device shipments would surpass 2.3 billion units globally by the end of 2015. Yet, many B2B and B2C document transactions that require signatures remain stuck in the era of fax machines, filing cabinets, and overnight mail. Adobe Sign, the e-signature solution offered by a company with a long-standing history and a strong commitment to delivering secure digital document technology, provides a low-risk, fast-ROI approach to securely digitizing your document processing.

For more information

Solution details: *https://adobe.com/go/adobesign*

Adobe

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

7/16