ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Sign Here: Electronic Signatures and the In-house Counsel

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***Not handwritten.*** Clicking a checkbox, entering a PIN or simply typing a name can constitute an electronic signature.
- ***Increasingly global.*** At least 50 countries have passed national legislation designed to regulate and/or promote the use of electronic signatures.
- ***Keep what you need.*** Electronic records can be ephemeral — and sometimes that's a good thing.
- ***Password protection.*** A password scheme can tie people to the document being signed.

Weeks of negotiation finally bear fruit, and all parties are in agreement and ready to sign. The only problem: Your signature authority matrix requires a VP signature and initials from the CFO and neither of them is in the office today.

Most of us have been in a situation like this, and the options for getting it signed were not attractive. Spend a small fortune overnighting the document to the CFO's Lake Tahoe condo? Instruct the vice president of sales to find a printer and fax machine in the business center at her hotel (confidentiality be damned!)? Or, wait however many days or weeks it takes for everyone to be in one place, at the risk of missing deadlines or losing the deal?

Fortunately, this is a problem of the past. Now there are numerous electronic signature tools available that enable your executives to sign from their laptop or mobile device, from anywhere they can connect to the Internet. The challenge for us, as in-house lawyers, is to guide our clients on the best way to take advantage of this technology.

What is an electronic signature?

In the United States, under the ESIGN Act, an electronic signature is defined as "an electronic sound, symbol, or 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." The definition varies somewhat in other countries, but as a general principle, **an electronic signature does not need to look like a handwritten signature.** Clicking a checkbox, entering a PIN or simply typing a name can all constitute an electronic signature so long as that action is tied to a record, and intended to function as a signature.

In practice, some common types of electronic signatures that you may encounter include:

- Clicking "I Agree" (or something similar) on a website in order to receive services or access content (these are known as "clickwrap" agreements);
- Signing with your finger or a stylus on a mobile device or signature pad (such as those at most grocery stores);
- Signing within a cloud-based electronic signature system;
- Typing your name and/or a PIN into an online form (such as the system used by the IRS for personal income tax returns); and

- Applying a thumbprint on a touch sensitive device.

From a legal perspective, all of these meet the definition of a signature, and each is equally valid. The main distinction between the various methods is the ease of use, and the type of evidence that will be available if the authenticity of a signature is challenged (more on this concept below).

Legal framework for electronic signatures – the United States

Beginning in the late 1990s, several states passed laws intended to promote the use of electronic commerce. Unfortunately, they did so in a manner that was inconsistent from state to state, and in some cases imposed technical requirements that made it much more difficult to sign something electronically than it was on paper. To try to promote consistency and ease of use, the National Conference of Commissioners on Uniform State Law (now called the Uniform Law Commission) adopted the *Uniform Electronic Transactions Act* ("UETA") in 1999.

Since its passage, UETA has been adopted in 47 states, the District of Columbia, Puerto Rico and the Virgin Islands. Only three states, New York, Illinois and Washington, have maintained their own independently developed laws addressing electronic signatures (which pre-date UETA), but all three have amended or interpreted them to be consistent with UETA in their effect.

Although UETA was adopted very quickly by a handful of states, some of the early adopters, most notably California, made exceptions to the scope of the law, which created inconsistency among the states. To address this issue, the federal government stepped in and passed the *Electronic Signature in Global and National Commerce Act* ("ESIGN") in 2000. ESIGN is modeled on UETA, and sets out the same key elements:

- A contract may not be denied legal effect or enforceability solely because of its electronic form;
- If a law requires a record to be in writing, an electronic record satisfies the law; and
- If a law requires a signature, an electronic signature satisfies the law.

ESIGN implements a national uniform standard for all electronic transactions and encourages the use of electronic signatures, contracts and records by providing legal certainty for these instruments when parties comply with its standards. There is no longer any doubt that contracts can be completed electronically, and the electronic records will satisfy writing requirements (e.g., the Statute of Frauds).

ESIGN preempts any state laws to the extent they aren't consistent with it, and is intentionally neutral in terms of the type of technology used (it even goes so far as to specifically preempt any state law that requires specific technology). ESIGN specifically notes that state laws adopted from UETA are not preempted by ESIGN, except to the extent they contain exceptions from the model law that are inconsistent with ESIGN.

Unlike the preemption language in many federal laws, the **ESIGN does not establish the floor for electronic signature laws — it establishes the ceiling.** States may not impose additional requirements on top of ESIGN that would create additional barriers to electronic commerce.

Special provisions for consumer transactions

ESIGN contains provisions intended to protect consumers engaged in electronic transactions. While

these provisions are not part of the original UETA, several states that adopted UETA after ESIGN was passed have incorporated them into state law.

At a high level, the goal of these consumer disclosure requirements is to ensure that consumers have access to any information they have a legal right to receive. Where a consumer would otherwise be entitled to receive information on paper, electronic information will satisfy the requirement, so long as the consumer:

- Is provided clear and conspicuous notice of the consumer's ability to receive the information on paper,
- Is provided with information about the hardware and software needed to access the information electronically, and
- Affirmatively consents to receive the information electronically.

Consumers must provide this consent in a manner that "reasonably demonstrates" that the consumer can access information in the electronic form that will be used to provide the relevant information. If there is a change to the hardware or software requirements to access the relevant information, which creates a material risk that a consumer could thereby lose access to the information, the consumer must be notified of the new requirements and of their right to withdraw consent to receive the information electronically. Consumers may withdraw consent to receive information electronically, but such withdrawal does not affect the legal effectiveness of any transactions already completed.

Although it is important to comply with the consumer disclosure requirements set out in ESIGN to the extent they apply, it is worth noting that ESIGN states that a failure to meet those requirements will not render any contract invalid or unenforceable.

Legal framework for electronic signatures – global

Electronic signatures also are widely used outside the United States, and at least 50 countries have passed national legislation designed to regulate and/or promote the use of electronic signatures.

As a general rule, common law countries, such as Canada, the United Kingdom and Australia, follow a similar approach to the United States, making electronic signatures broadly equivalent to handwritten ones and not requiring or giving preference to any particular technology.

By contrast, most civil law countries, including most European Union member states, and much of Asia and Latin America, have adopted a "two-tier" approach, in which "simple" electronic signatures cannot be invalidated solely on the grounds that they are electronic, but signatures meeting specific statutory criteria, including the use of PKI technology, and sometimes the use of government-approved certificate authorities, have special legal status. Signatures that meet the requirement for this higher tier are granted a presumption of authenticity, and may be required in order to do business electronically with government actors.

Although the different treatment in civil law and common law countries can cause confusion, there are a couple of general statements that can be made about electronic signatures around the world:

- If parties to a commercial transaction agree to do business electronically, their agreements will not be invalidated solely on the ground that they were formed electronically; and
- Electronic records, including electronically signed documents, **are permitted** as evidence

(subject to the relevant rules of evidence, such as the need for authentication).

Electronic Signature vs. Digital Signature

While it is tempting to use the terms “electronic” and “digital” interchangeably, these are terms of art with very specific meanings in the context of electronic and digital signatures.

Electronic signature is a technology neutral concept that includes any sound, symbol or process that performs the function of a signature. It is sometimes called a “simple” electronic signature.

Digital signature refers to a signature based on specific cryptographic technology called Public Key Infrastructure (PKI). It relies on the use of paired cryptographic keys, one of which is kept secret, and the other maintained and made public by a Certificate Authority. Digital signatures are more commonly used in civil law countries, such as those following the European Directive on Electronic Commerce, under which they meet the definition of “advanced electronic signatures.”

Key considerations for in-house counsel

Think about proof

As with any contract, simply having a signature may not be enough to enforce the agreement. If the counterparty claims that the signature is fraudulent, or that the content of the document has been changed after the fact, you may need to convince a judge or jury that the version presented is genuine.

This is not to say that you need to keep elaborate records of every transaction, or require a cumbersome authentication process for everyone who signs a contract. Instead, consider the type of transaction, and put measures in place that strike the right balance between ease of use and support for potential disputes.

- **Password protection.** For people whose identity you already know (such as your employees), you can often use a password scheme to tie them to the document being signed. When relying on a password to identify someone, make sure they are the only ones who have access to sign in their name, and that the document can’t be modified after the fact by anyone else.
- **Clickwrap agreements.** A clickwrap agreement may be a good option for high volume agreements like your online terms of use. If you use this approach, you probably won’t want to save a separate PDF copy each time a user agrees to the terms. Instead, make sure you understand what kind of evidence will be available to demonstrate that the user agreed to the terms through your online process. This will typically be a record of the time and date that the user took action, their IP address and whatever information they provided in connection with accepting the terms. You may want to periodically document the process with screenshots.
- **Mirror your paper process (or improve it).** People often get hung up on potential problems with electronic signatures, forgetting that the same problems exist when signing on paper. If you send a paper copy of a sales agreement to the office of your prospective customer, and it arrives back two weeks later with a scribble on the signature line, most of us wouldn’t

question whether that was sufficient proof. A document delivered via email may actually provide much better proof, since an email is generally unique to a specific person, rather than an entire office.

It is worth noting that although there are potential pitfalls with an electronic signature process, it is often still superior to a paper-based system from an evidentiary standpoint. An electronic signature will frequently be associated with an email and/or IP address or other elements associated with the signer, whereas a contract sent by mail will only be associated with a physical location where others may reside and a written signature which may be forged.

Permissive vs. Proscriptive Legislation

You may be wondering, in light of the legislation clearly aimed at promoting electronic signature, why some entities will not accept electronically signed documents.

ESIGN and UETA, as well as most of their international counterparts, are permissive, not proscriptive. They ensure that if parties to a transaction choose to do business electronically, they will not be denied the ability to do so. However, **no one is required to do business electronically** under these laws.

The use of electronic signatures is growing rapidly, but there are still people, companies and government agencies that are reluctant to do business electronically, and it is their prerogative to decline to do so.

That said, there are indications that more conservative entities are becoming open to electronic signatures. For example:

- The IRS reports that nearly 120 million US taxpayers filed their 2013 returns electronically.
- The Small Business Administration reports that in 2013, 92 percent of all 7(a) loan transactions (the SBA's most common type of loan) were completed electronically.
- Many banks, including Bank of America and US Bank, accept electronic signatures on a variety of documents.
- Most US local court rules permit electronic signature of pleadings, and often even judges' orders.

Records management and retention

We already live in the world of email, cloud storage and ediscovery. Electronic signatures may not really present new issues in this arena, but they do highlight the need for thoughtful document management. Some specific items include:

- **Keep what you need.** Electronic records can be ephemeral — and sometimes that's a good thing. Many of us struggle to prevent our clients from keeping a copy of every email they've ever sent, for fear of having to disclose terabytes of data in response to a discovery request. However, if you implement policies to combat that, such as automatic deletion of old email, make sure you don't throw out electronic records that you need, such as evidence of an offer

or acceptance to contract terms that were completed by email.

- **Know where your electronic documents are stored**. Document management in many organizations is very fragmented, particularly with the proliferation of cloud-based storage. Some teams may use file servers, while others use collaboration tools like Sharepoint, box.com, Dropbox, etc. It is important for you to be able to find documents, particularly contracts, so you can monitor your obligations and address disputes or discovery requests.
    - **Try to centralize storage of documents you care about.** This may mean purchasing a document management system (there are many options out there, offering a variety of enticing features like integration with your CRM, ticketing system, etc.), or just choosing an existing location within your IT system that all relevant parties can access.
    - **If you are using a cloud-based system to electronically sign documents, the document is likely stored in that system for at least some amount of time.** This can be a benefit in terms of having access to the document, but it also creates a second (or third, or tenth) location that you may need to consider when searching for responsive documents in discovery.

Privacy and data security

It goes without saying that privacy and data security are important considerations when converting any process from paper to electronic. That said, don't let concerns about privacy and data security stop you from improving your process. An electronic signature process, when implemented correctly, can be just as secure, and potentially much more so, than a paper process. Electronic documents can be encrypted, password protected and subject to audit logs that allow you to see who has accessed them. You have many more options for maintaining and monitoring their security than you do for pieces of paper in a drawer.

When looking to implement electronic signatures, consider the security level that's appropriate, and look for systems or vendors that understand the importance of the issue, and that can offer assurances about information security. If you have a security team, make sure they are involved in selecting any vendors that will store or access confidential information (whether it involves electronic signatures or not). Make sure your staff understands their responsibility to protect confidential information, and implement policies that reduce risk, such as requiring a password on any mobile device that can be used to access confidential information.

How do corporate legal departments benefit from electronic signatures?

- Reduced use of paper, mail, overnight courier services, etc.
- Documents can be signed remotely — no more waiting around the office to sign.
- Counterparts can be sent simultaneously to multiple signers, and easily tracked and kept together electronically.
- Electronic systems allow you to track more information about the signing process, such as when and how often a document was viewed before being signed, where the signer was geographically located when they sign, etc. Some systems even allow you to see the status of a document in real time as it is routed for signature.
- Electronic systems can also include required fields, so contracts cannot be completed unless all of the required elements are present. You won't have to waste time dealing with contracts that come back signed, but with key information like the effective date missing.

Overcoming resistance

Many people, perhaps especially lawyers, are resistant to change. We tend to be skeptical about anything new. It is certainly appropriate to be thoughtful about any new process, particularly one that impacts many of our most important transactions, but we should not apply a higher standard to electronic signatures than we do for handwritten ones.

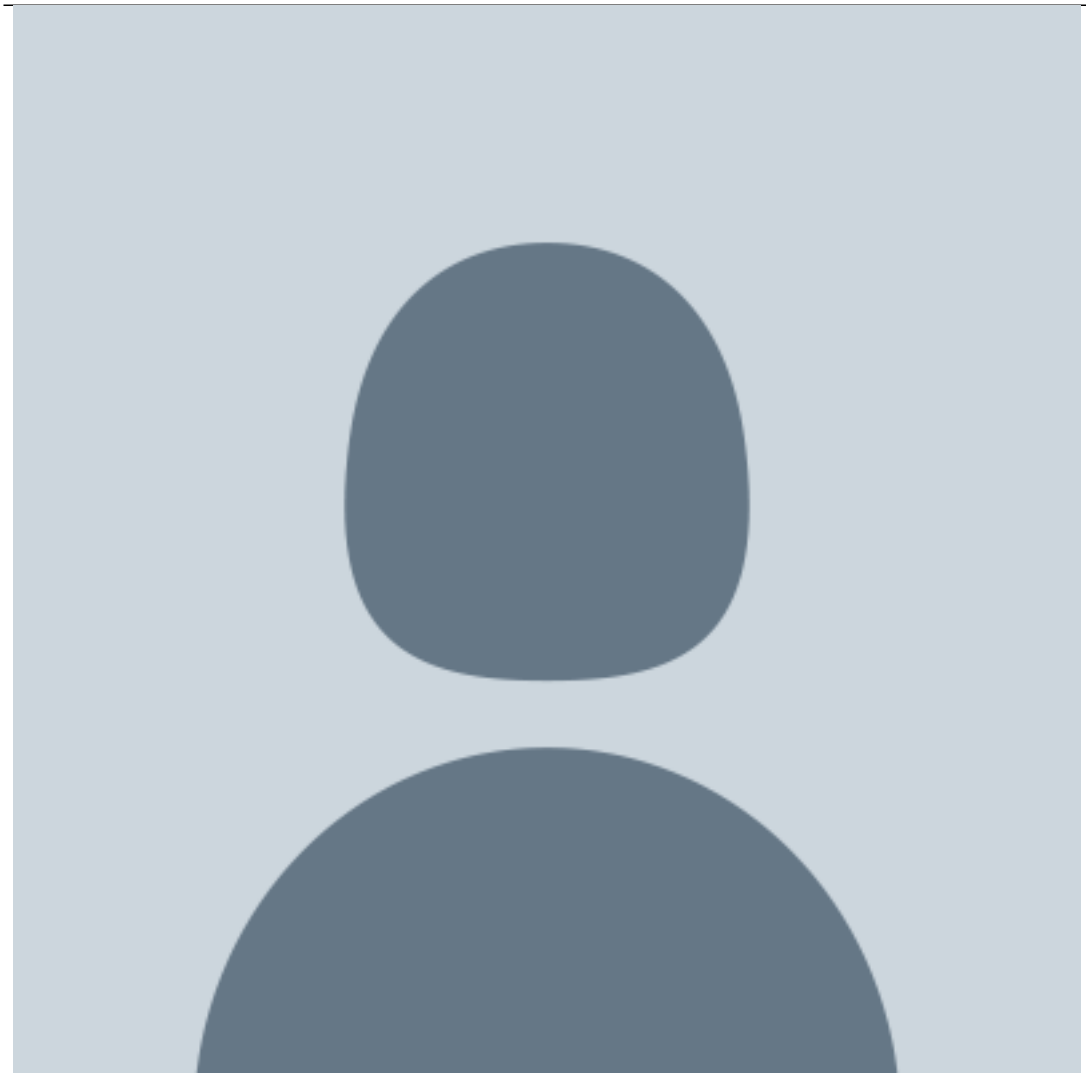
During a recent talk with a group of in-house lawyers about implementing electronic signatures, one of the lawyers expressed concern that a document sent to a company for a signature might be electronically signed by a person who did not have authority to bind the company.

This is obviously a valid concern, but the concern has nothing to do with the signature being electronic. The same problem is presented by his existing process, which involves routing multiple paper copies of the document within his own company, then sending them to the counterparty in the mail.

Similarly, I am often asked how we can be sure that the person whose signature appears on the document is really the one who signed it (and not someone else signing their name). Well, how do we know that now? Implementing electronic signatures can present an excellent opportunity to reevaluate our practices, but we should avoid standing in the way of improvements simply because they fail to solve problems that we have already determined we can live with when they occur on paper.

Electronic signatures present one of those rare opportunities for us to improve the service we provide our customers, and also make our own lives easier. That is true client service.

Rachel Stoermer



Senior Corporate Counsel

DocuSign

She focuses on issues surrounding electronic signature legality and adoption.