ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

The Challenges of Electronic Signature Implementations

Technology, Privacy, and eCommerce

Electronic signatures have been legal and enforceable in the United States since the passage of the ESIGN Act in 2000. Electronic signatures provide an enormous opportunity for in-house counsel to facilitate speed, efficiency and reliability in the contracting process. Yet, many attorneys who have been trained in the "sign-it-in-blue-ink" school of signature gathering still regard electronic signatures with a wary eye. They are not alone.

In fact, on July 14, 2014, three of the original proponents of the ESIGN Act — Senators Ron Wyden and John McCain, and Representative Anna Eshoo — wrote to Commerce Secretary Penn Pritzker, "concerned about the extent of the adoption of electronic signatures within the federal government." They also wrote to "request a report on the state of this Act's implementation by federal agencies ("Lawmakers want more e-signatures"). These lawmakers were asking why the federal government has been so slow to adopt electronic signatures — legislation that was designed to help them streamline their processes.

Yet, the federal government's response is not unusual. The conundrum of e-signatures in 2014 seems to be that everyone in the legal community knows that they are legal and enforceable in the United States, everyone recognizes that they represent a tremendous opportunity to gain speed and efficiency in contracting, many have even implemented limited pilot projects, yet some unease appears to prevent really robust adoption. Let's take a look at why that might be.

Signature types

Written signatures are, of course, the handwritten signatures we are all familiar with.

Digital signatures — sometimes also called authenticated electronic signatures or (in the EU) advanced electronic signatures — use secure public/private key encryption to authenticate the identity

of the signer, as well as the integrity of the signed document. They are highly secure but also quite cumbersome to implement and use since each participant in the process must first obtain a digital certificate or physical token from a certificate issuing authority. This requires presenting oneself in person and submitting government-issued ID and biometric data (e.g., retinal scans or fingerprints). While this makes sense for parties who have regular transactions with one another, it is an unacceptable hassle to most consumers and small businesses.

Under the ESIGN Act, *electronic signatures* are any electronic symbol reasonably related to a contract created with the intent to sign that contract. This can range from electronically checking a box that indicates acceptance, typing one's name into a data field or hitting an "Agree" button to a software license. The great advantage of electronic signatures is that they can be used by anyone without having to first obtain a digital certificate. Because of their speed and ease-of-use, it is electronic signatures that represent the greatest opportunity to speed up contracting processes for the largest number of businesses, governments and individuals.

This uneasiness seems to arise from the belief that written signatures are trustworthy and reliable and the fear that electronic signatures are new and untested. Neither of these beliefs is accurate. Often, our reliance on written signatures is not warranted. In-house counsel know this all too well. And here is what we see all too often: An agreement is finalized by phone or email. The agreement is sent via email, fax or regular mail to a provided address. Hours pass. Days. Weeks. The seasons flicker by, and at last, the contract is returned. Upon opening the envelope, one sees a document that *appears* to be the version sent, *possibly* from the same address, email address or fax number that it was sent to, with a scrawl that *might* be from the person whom you *believe* has signing authority in what *may or may not* be her actual signature. Yet, this is the process on which we rely.

We find ourselves in an era where document generation, editing, exchange, routing and archiving are all done electronically. It is only for this single act of signing that we are suddenly transported to the pre-digital age, print out a hard copy, pull out our ink wells, flourish our quills and sign. One might reasonably assume that counsel would flee such an unreliable process, yet many do not. Why?

Partly, it's because many still see electronic signatures as new and untested. When I talk to groups about this topic, I often ask if anyone can guess when the United States courts first held that an electronic acceptance was binding. Some guess 2000. Some guess 1985. An occasional daring soul will offer 1972. No one guesses 1869.

Yet in *Howley v. Whipple* (48 N.H. 487 (1869)), the New Hampshire Supreme Court did just that. It determined: *"It makes no difference whether [the telegraph] operator writes with a steel pen an inch long attached to an ordinary penholder, or whether his pen be a copper wire a thousand miles long. Nor does it make any difference that in one case common record ink is used, while in the other case a more subtle fluid, known as electricity, performs the same office."*

Still, many resist electronic signatures simply because they have never executed one. It is entirely new behavior. Studies into how we perceive risk consistently show that we dramatically overestimate the risk of anything new. Uncertainty and fear of the unknown works to undermine our usual risk

assessment process.

Yet, compared to written signatures, e-signatures are much safer and easier to use. Contracts can be signed from tablets and smart phones, allowing executives to sign documents while traveling or on vacation. This eliminates the common problem of business grinding to halt while key signatories are tracked down. Further, e-signatures allow all involved to maintain visibility into the real-time status of where each document is in the signing process. Digital rights management can be enabled in documents, giving counsel peace of mind that no alterations were made in the final versions.

That said, in-house counsel can take some basic steps to move smoothly to electronic signatures. First, always be sure to obtain consent. The contract must contain a provision stating that all parties to that contract agree to sign electronically. Second, one must always retain an electronic copy of the contract in accordance with usual departmental practice. Third, it is advisable to retain a copy of the contract's audit log. Most — if not all — electronic signature solutions generate audit logs of the contract's signature path — from sender to signer, back to sender and then to archive, all while recording the times, IP addresses and relevant email addresses. Finally, an unaltered, fully executed, complete electronic copy of the contract should be sent to all parties for their reference and archiving.

Electronic signatures have become one of the primary mechanisms for executing agreements. Counsel who use them not only find them a safe, effective way of doing business, but often, they also remark that they could not imagine returning to paper-based processes. For those who have not moved to electronic signatures, all that is required is for one to swallow hard and make the leap.

Dan Puterbaugh

Legal Lead

Adobe Sign

Dan Puterbaugh is legal lead for Adobe Sign, Adobe’s electronic signature solution. His writing has appeared on ACCDocket.com, and in Legal IT Insider and CMSWire.