Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The E-Sign Act: 18 Years And All Grown Up

By **August Heckman** (June 28, 2018, 11:22 AM EDT)

August Heckman

On June 30, 2000, President Bill Clinton signed the "Electronic Signatures in Global and National Commerce Act," or the E-Sign Act, which, together with the Uniform Electronic Transactions Act, or UETA,[1] establishes that electronic signatures may not be denied legal effect solely because they are in electronic form. For employers, this means no longer having to track down and obtain — and then retain — hundreds or thousands of traditional wet signatures. Indeed, many employers have completely digitized their new employee onboarding process, human resource document systems, and have expanded into using electronic signatures for employment agreements — including noncompetes and arbitration. As the E-Sign Act reaches the age of maturity after being tested in the courts, and as more employers adopt or broaden their use of electronic signatures, now is a good time to review the basic requirements and lessons learned from the developing case law.

Basic Requirements

At the very least, an electronic signature must be unique and verifiable so that it can provide the authentication and nonrepudiation benefits of a handwritten signature. The basic requirements include:

- Clear intent to sign — signatories must show clear intention to electronically sign an agreement.
- Opt-out provision — signatories should be given an opportunity to opt-out of signing an agreement electronically.
- Consent — there must be consent to do business electronically and this can be buttressed by including a consent clause in the agreement or employee handbook.
- Access to the signed document — all signatories should receive a fully executed copy of the agreement.
- Retention — the records should remain accessible in a form that permits accurate reproductions for anyone entitled to their access.

While there is no specific requirement as to what constitutes an electronic signature under federal law, it 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."[2] This has translated to anything from unique codes, to a checkbox, to even biometric data. As such, as for any signature, the ability to show that a document was signed by the purported signatory, that the signature is authentic and that the signature has not been tampered with are key requirements to uphold.

In the employment context, courts have fleshed this out to require employers to show:

- The employee was provided with unique login credentials and a password which the employee may change on his or her own accord;

- The document at issue is protected by security and privacy measures, and it can be linked directly with the employee's login credentials, thereby showing that the employee's unique credentials are directly linked with the signature; and

- The employee must affirmatively click through various electronic steps in order to place his or her name on the document.

Unfortunately for employers, current and former employees often suffer from amnesia in challenging the authenticity of their very own electronic signatures by claiming that they do not remember signing — or that they never even saw — the agreement in the first place.

Developing Case Law

While the case law is far from robust, there have, indeed, been challenges to electronic signatures. Because federal law removes any viable challenge to an electronic signature simply because it is electronic, most challenges have fallen into two categories: (1) authentication or (2) ignorance. In Espejo v. Southern California Permanente Medical Group, the California Court of Appeals for the Second Appellate District dealt with the former and clarified what an employer must show in order to authenticate an electronic signature for arbitration agreements. There, Espejo electronically signed an arbitration agreement prior to joining the defendant, Southern California Permanente Medical Group, as a physician. Approximately three years later, he sued for wrongful termination and whistleblower retaliation. The defendant moved to compel arbitration. Espejo opposed by contending that the signature was not authenticated as his own. Specifically, he argued that he did not recall ever signing electronically or otherwise and stated that he customarily reviewed documents before signing them.

The trial court denied the motion to compel, grounding its decision on the fact that defendant failed to provide a timely declaration in which its systems consultant elaborated on the signature process. The defendant did, however, submit a declaration as a supplement after filing its motion. Ignoring the untimely declaration, the trial court was particularly concerned that the defendant lacked any evidence that the signature was the plaintiff's and not that of another individual.

The California Court of Appeals reversed. Critical to the reversal was, in fact, the systems consultant's declaration that the defendant submitted as a supplement to its motion to compel because it thoroughly described its electronic review and signature process for employee agreements. Among the details the defendant provided were: the security precautions regarding how an applicant's unique username and password was transmitted; the specific steps any employee would need to take to actually affix their name on the signature line of the agreement; and how an employee may change his or her password — a required step in proceeding to the employment documents. As a result of this detailed description, the appeals court was satisfied that the defendant met its burden of proving that

the signature was, indeed, that of the plaintiff's.

The Third Circuit recently dealt with the "I didn't read it" argument in ADP v. Lynch and ADP v. Halpin.[3] There, the defendants worked in sales at ADP and throughout their respective tenures were offered incentive stocks awards based on positive performance. ADP required all employees to electronically "sign" their stock awards by checking a box indicating they read all related documents, which, in turn, incorporated an agreement not to compete. Further, the award agreement expressly stated that acceptance of a stock award was conditioned on assenting to the agreement not to compete. However, upon termination of their respective employments, the defendants began working for the plaintiff's direct competitor.

As such, ADP sued for breach of the agreement not to compete. The district court entered a preliminary injunction enjoining the defendants from soliciting ADP's clients. On appeal, the defendants argued that the box they checked when accepting the stock award only indicated that they read the documents, but did not specify the particular terms of the documents, which they contended they did not remember reading. The Third Circuit rejected this argument entirely — not only did the defendants admitted that they checked the box stating they had read the documents, ADP showed that after checking the box, defendants had to enter their personal passwords and affirmatively click "accept" or "reject."

Lessons Learned

Whether an employee or former employee is bound by an electronic signature depends on whether or not he or she affirmatively engaged in an electronic transaction. This will be determined by the context and circumstances surrounding the transaction. To that end, there are some safeguards an employer may take to combat potential litigation and other pitfalls:

- Memorialize policies surrounding electronic signatures in writing, such as in a handbook provision;
- Ensure employees affirmatively agree to complete any employment documents using an electronic signature;
- Provide employees with a unique username and password to access the employer's system;
- Ensure that each electronic signature is accompanied by an accurate date and time stamp, along with the IP address of the device the employee used to sign the document;
- Notify employees that they are required to read and review every document;
- Provide ample time for employees to review and sign documents; and
- Contemplate drafting a template declaration that details the specific safeguards in place and the steps an employee is required to take to affix an electronic signature.

While the E-Sign Act has ripened, some formative issues remain but can be counteracted with some simple adjustments and modifications. Employers can easily utilize the efficiency of electronic signatures in their hiring and retention practices and employment agreements without worrying about potential litigation if careful steps are taken to maintain security protocols for unique employee credentials. It is also key that employers understand the electronic signature laws of all states they maintain business

operations in, as some states follow the UETA or have their own version which may differ from the E-Sign Act.

August W. Heckman III is a partner-elect at Morgan Lewis & Bockius LLP.

[1] Adopted by 47 states, Washington, D.C., Puerto Rico and the U.S. Virgin Islands, its purpose is to integrate state laws concerning retention of paper records and the validity of electronic signatures. Washington, Illinois and New York have not adopted the UETA, however, similar legislation that governs how electronic transactions are handled has been enacted in each of these three states. Thus, since state laws may vary, it is important to check each state's regulations for further information. While this particular article will only focus on the E-Sign Act, it is important to note that both the E-Sign Act and UETA do not govern wills, trusts and a number of other transactions that are managed by the court system.

[2] 15 U.S.C. § 7006(5) (2000).

[3] ADP v. Lynch and ADP v. Halpin, Nos. 2-16-cv-01053 and 2-16-cv-01000 (3rd Cir. Feb. 7, 2017).