FEATURE

Electronic Signatures Are Enforceable—If You're Careful

by Joseph Kanfer, Woolford Kanfer Law, P.C.

It used to be that the last step in finalizing a contract or change order was putting pen to paper and signing it. But as computer technology becomes ever more pervasive in the construction industry, contract documents and signatures are increasingly exchanged by electronic means like email or even signed on a computer itself. Electronic signatures can save time and money and are legally binding if certain requirements are followed. The purpose of this article is to explain the basic requirements of enforceable electronic signatures, help you avoid some of the potential pitfalls of electronic signatures, and illustrate how good practices can reduce the risk of running into problems.

Electronic Signatures Laws

The law on electronic signatures is complex and is covered by both federal and state laws, which are not always consistent. Under federal law, electronic signatures are governed by the Electronic Signatures in Global and National Commerce Act, known as the ESIGN Act. Additionally, all 50 states have adopted their own laws governing electronic signatures. Most states, as well as the District of Columbia, have adopted a law called the Uniform Electronic Transactions Act (UETA). New York, Illinois, and Washington have not adopted UETA and each have their own laws concerning the validity of electronic signatures. Therefore, you need to check with your legal counsel to confirm the requirements of each state.

The ESIGN Act and UETA both provide that electronic signatures are generally enforceable to the same extent as traditional ink signatures. Under both the ESIGN Act and UETA, a valid electronic signature can be any "electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record." Thus, an electronic signature could include anything from an image of an actual written signature to somebody typing her name on the signature line of a contract.

The form of the electronic signature does not matter as long as the requirements of the applicable law are met. The ESIGN Act and UETA both share several general requirements. First, an electronic signature is valid only if the party whose signature is on the document intended to execute the document. Second, the parties to the transaction must consent to do business electronically. In most business-to-business commercial transactions, this can be shown by the circumstances surrounding the transaction. (Note that if your business offers services to consumers, there are additional disclosures that are required which are not discussed in this article.) Third, the electronic document must be in a form that can be retained and accurately reproduced for later reference by the parties. The most commonly used format to exchange electronic documents, Portable Document Format (PDF), is well-suited for accurately reproducing documents (and PDF files can even be protected against tampering using encryption technologies). Finally, the electronic signature must be shown to have been "the act of the person" who signed the document.

Unique Pitfalls

These requirements may seem easy to meet, but they can create loopholes that a company can exploit to get out of a contract. For example, in a Kansas court case called Kerr v. Dillard Store Services, an employee sued her employer for discrimination. The employee was required to sign an electronic agreement to arbitrate any employment disputes when she was hired. This process required her to log-in to the company's computer system using her social security number and a password she had created and then click a button indicating that she accepted the agreement. The employee then received an email confirming her signature. Based upon this electronically signed agreement to arbitrate, the employer sought to compel the employee to arbitrate her discrimination claims.

The court ruled that the signature was not enforceable because the employer could not demonstrate that the signature was "the act of" the employee. The court found the employer did not have adequate procedures to maintain the security of employee passwords, to prevent other people from accessing the employee's account, or to determine whether electronic signatures were genuine. The employee's signature was therefore not enforceable and the discrimination claim was not subject to arbitration.

A California state court came to the same conclusion in Ruiz v. Moss Brothers Auto Group, Inc. In that case, an employee filed a wage claim against his employer. Just like the employer in the Kerr case, this employer required employees to log-in to the computer system with their unique username and password and electronically sign an agreement containing an arbitration provision by clicking a button. Seeking to get into court and avoid arbitration, the employee testified that he did not

recall signing the arbitration agreement, and the employer was unable to explain how the company's computer system stored the signature and generated the document with the arbitration clause. The court therefore concluded the employer had not shown the signature was "the act of" the employee.

Showing that the person whose signature appears on the document is not the only difficulty in enforcing electronic transactions. In another California case, *J.B.B. Investment Partners, Ltd. v. Fair*, a court considered whether a settlement agreement that had been circulated by email was enforceable. In that case, an investor in a company that built apartments claimed that the owner misled the investor and threatened to sue for damages. The investor sent a proposed agreement to the owner to settle the investor's claims. The owner wrote back in an email "I agree" and typed his name at the end of the email. The owner later refused to honor the settlement agreement. The investor sued in court to enforce the agreement, but the owner claimed that the electronic signature was not valid because he did not intend to sign the settlement agreement. The court ruled the agreement was not enforceable because it found typing "I agree" and the owner's name did not show intent to sign the agreement. Without a showing of intent, the signature was not valid.

Electronic signatures can also create unique issues of tampering with documents. For example, imagine a subcontractor prepares a proposal for a project and the estimator types his name on the signature line. The estimator then sends the proposal to the general contractor as a PDF. However, the general contractor modifies the PDF so that overall bid price is 10 percent lower than the proposal before typing a signature on the altered proposal and sending it back. The subcontractor would then be in the position of having to show that the subcontractor doctored the PDF, which can turn into the digital equivalent of "he said, she said."

While situations such as these should be kept in mind as potential worst case scenarios when conducting business electronically, they are a relative rarity considering how common electronic document exchanges are. In the vast majority of cases, there is no dispute as to whether an electronic signature on a document is valid. Moreover, the risks associated with electronic transactions can be mitigated though implementation of sound practices and procedures.

Making Electronic Signatures Valid

Problems with electronic signatures generally arise when businesses do not use care when implementing procedures for digital transactions. In the Kerr case, the computer system did not have sufficient security measures. In the Ruiz case, the company's employees were not sufficiently knowledgeable about the system to explain how it worked. In the Fair case, the parties to the contract failed to clearly establish what would constitute an electronic signature on the contract. These problems could have been avoided by using proper software and sound procedures.

There are a number of computer programs and services that address the pitfalls of electronic signatures. Services such as DocuSign and Adobe Sign are designed to create certainty as to the identity of the party signing a document through security procedures, as well as demonstrating that the party clearly intended to sign the document. Instead of merely typing in the signer's name on a PDF document, these services require the person signing the document to go through a process to add a signature to a document once the document is finalized, much like signing a document with an ink signature. Unlike traditional ink signatures, however, these digital signatures contain features that allow a reader to instantly determine whether a signed document has been altered. However, using the correct software is just part of a responsible implementation of electronic signatures. Businesses must also implement processes and procedures to ensure that the software is used properly and consistently, such as including provisions in contracts indicating exactly how contracts can be signed electronically.

Digital documents with electronic signatures will continue to become increasingly common as business owners and consumers become more comfortable with digital commerce. A well-planned and intelligently executed implementation of electronic signatures can save companies time and money, while also ensuring that electronic contracts and other documents remain legally enforceable just as if they were on paper.

Joseph Kanfer, Esq., Woolford Kanfer Law, P.C., is an attorney in Lancaster, Pa., who represents subcontractors and other construction professionals. He can be reached at (717) 290-1190 or jkanfer@woolford-law.com.