infotech

WHITE PAPER

Are electronic signatures enforceable by law?

infotech

What is a 'signature,' anyway?

In the commonly understood meaning of the word, a 'signature' is a person's name or mark written by that person, or at the person's direction. A more technical definition of the word in the commercial law context is "[a]ny name, mark, or writing used with the intention of authenticating a document."1 On the internet, a common form of signature is a checkbox that a user must check before finalizing a purchase. At an ATM, a person's PIN is a signature. And, of course, an "X" can be a legally binding signature. Electronic signatures are no different – the issue of whether or not a 'signature' is able to be relied upon legally has never been the definition of a signature (or even legal prohibition); rather, the issue is a combination of the assurance of the identity of the signer, the signer's intent to be legally bound, and the assurance that the signer knows what is being signed.

What is an 'electronic signature?'

The most widely used definition of an electronic signature is "an electronic sound, symbol, or process attached to or logically associated with a document and executed or adopted by a person with the intent to sign the document."2 This definition is from the Uniform Electronic Transaction Act (UETA), which has been adopted as law by 47 of the United States, and the three states that have not adopted UETA (IL, NY, WA) have substantially similar definitions. Although the UETA is a relatively new uniform act, electronic signatures have been recognized as legally binding in the United States since the time of the American Civil War, when legally binding contracts were made over the telegraph in Morse code. A faxed document with a signature is an electronic signature, as is a message left on voicemail.

The Uniform Electronic Transaction Act and similar laws: legal authority.

It is arguable that an electronic signature qualifies as a legally binding signature without the help of any legislative action. As mentioned above, only three states have not enacted the UETA. However, every state has enacted legislation that ensures the legality of certain aspects of electronic transactions, and the UETA states specifically the following principles (UETA § 7):

a. A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
b. A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.
c. If a law requires a record to be in writing, an electronic record satisfies the law.
d. If a law requires a signature, an electronic signature satisfies the law.

UETA § 9 discusses the attribution and effect of electronic records and electronic signatures:

a. An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of efficacy of any security procedure applied to determine the person to which the electronic record or signature was attributable.
b. The effect of an electronic record or electronic signature attributed to a person under subsection (a) is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement, if any, and otherwise as provided by law.

What this means to parties who are considering electronic transacting as a way of doing business is: if we agree on the electronic method of the transaction, including security and authentication methods, we can be assured that our contract will be legally enforceable even though there is not an ink signature. This is directly comparable to how we do business in person as a society. Some contracts are made with a handshake. Some contracts are made with a simple exchange of paper money for goods. Some contracts are written down on paper and require signatures of everyone agreeing to the contract. The common principle is that if everyone involved agrees that a contract is made, it is made. The proof of that contract is the only thing that changes – if a merchant sells some everyday goods to a consumer, that consumer typically does not have to sign a contract. But, that merchant would be foolish to give the goods away for a handshake.

Will a document electronically signed with an Infotech Digital ID be recognized in court?

A wet ink signature on a page is only acceptable as proof of thte existence of an agreement because of the long-standing tradition of doing business in that way. Contracts for many years were memorialized almost exclusively on paper, and a person's signature was considered to be enough to assure all parties of the identity of the signer, the intent of the signer to be bound by the contract, and that there is an agreement to the terms of the contract. The fact of the matter is, though, that almost no laws specifically require wet ink signatures or define a signature as a wet ink signature – notable exceptions are notary statutes and statutes governing the creation of wills, trusts, and codicils. In the law of contracts, however, there is no relevant principle that requires a signature (if a signature is required at all) to be a person's name signed in ink by that person. The actual method of signature is left up to the parties to the contract to decide. So, in a sense, the signature is not as important as the security and authentication measures that are behind that signature.

If an electronic signature is at issue in a court proceeding, parties relying on that signature need to be assured that the contract or signature will be recognized as authentic by the court – this is the ultimate purpose of any signature requirement. Here are some considerations that will be taken into account in the event that a signature created with an Infotech Digital ID is at issue in a court of law:

- **Proof of Identity** – Infotech's proprietary Digital ID process requires the Infotech Digital ID holder to submit notarized acknowledgement to Infotech of the holder's identity. The strength of this acknowledgement is as strong as the state laws of the notary's jurisdiction, and Infotech manually verifies the sufficiency of the notarial act for each applicant. No Digital ID is functional before the integrity of the process has been individually approved, and there is no use for the Infotech Digital ID apart from Infotech's services.

- **Control of the Digital ID** – As with most commercially available digital signature creation systems, an Infotech Digital ID employs a secure cryptographic key pair. This technology relies upon the Digital ID holder to keep the holder's private key secure. This key resides on the holder's computer. Any use of the Digital ID is thus attributable to the Digital ID holder or the holder's authorized agent.

- **Proof of Integrity** – The Digital ID is used to digitally sign the holder's signature, and any content logically associated with that signature, via a cryptographic method that can only be decrypted by the public key portion of the holder's Digital ID. The public key can be freely transmitted, as its only use is decryption and verification of the encrypted message. This method of encryption allows the recipient of the message and the public key to be assured of not only the identity of the signer, but also that the message itself has not been altered in any way. Thus, all the contents of the digitally signed message can be attributed to the holder of the Digital ID.

Does my agency have the authority to accept signatures created with an Infotech Digital ID?

The answer to this question is probably yes. In most cases, the requirement of an ink signature is simply a holdover from the days not so long ago that paper documents were the only widely accepted means of memorializing a contract. While electronic signatures are recognized as valid in every state, the primary purpose of the signature on most contracts is to indicate that the signer agrees to the terms of the contract. The ink signature is commonly accepted as the method of finalizing a contract, but usually it is not in any way the sole legally enforceable means of finalizing a contract.

A state or local government agency may have a statutory obligation to accept signatures on certain documents, but recall that, according to the UETA, if a law requires a signature, an electronic signature satisfies the law. It is more likely that a prohibition exists on a state regulatory level, which may or may not be able to be interpreted in such a way that would allow an agency to accept electronic signatures. It is also to significant that a document which requires a notarization makes an electronic signature process more difficult, as a notarial act generally requires a person to personally appear before the notary public, and the notary public is generally by statute required to provide an ink signature. However, these types of prohibitions are the exception, rather than the norm.

This document is not legal advice, and is far too brief to provide answers to all of the questions that must be answered when making a complete determination on whether or not electronic signatures are always a legally sufficient method of contract execution. If there are questions about whether or not an agency is able to accept electronic or digital signatures on documents, it is important for that agency to seek the advice of their legal department, counsel, or the Attorney General of the state. Infotech welcomes the opportunity to provide further information to the agency or to any agency's legal counsel with information that would help the appropriate party reach a well informed decision on the matter of Infotech's electronic signature and digital signature process.

For more information, please contact the Infotech Legal Department:

Benjamin C. Bourdon, Esq., Legal Counsel
(352) 381-4400
benjamin.bourdon@infotechfl.com

Carole DuVal, Director of Corporate Affairs
(352) 381-4400
carole.duval@infotechfl.com