Datawitness®
Online Witnessing and Archiving

Electronic Signature: Increasing the Speed and Efficiency of Commercial Transactions

Signatures make the world go round. In other words, we need to commit and receive commitments from others in order make commerce work. A signature is the embodiment of a commitment by an individual or organization. The process of creating a contract and signing a document has a long history. Yet providing or receiving a signature can be a challenge and has not changed much for centuries.

The Internet allows us to communicate better and faster, but has it enabled us to improve the way we execute contracts? We believe the answer is yes. An established and accepted framework of legislation provides the much needed assurance that a signature obtained online via the Internet and World Wide Web, known as an e-signature, has the same validity and enforceability as a physical, ink-on-paper signature (known as a “wet signature”).

The Speed of Business Demands New Methods for Exchanging Contracts and Obtaining Signatures

The pace of business is faster now than ever before. People expect faster turnarounds and responses in commercial transactions requiring a two-way flow of paperwork. Businesses and organizations are under pressure to get more done in less time with fewer resources. With the ubiquity of computers and the Internet comes increased access across distance and a new impatience. People are not willing to wait for paper to travel between parties for signature. The main factor holding back the development of widespread electronic signing processes was lack of support in law for electronic signature.

That barrier has been removed. E-signature is growing in popularity and adoption as an alternative to traditional, ink on paper methods for exchanging

and executing documents requiring signature. Let's review the legal background for electronic signature.

The Legal Basis for Online Signing is Almost a Decade Old But E-Signature is Still a New Idea to Many

In 2000, President Clinton signed into law the Electronic Signature in Global and National Commerce Act (E-SIGN Act). E-SIGN became effective in the United States on October 1, 2000. E-SIGN implements a national uniform standard (the 'floor') for all electronic transactions and encourages the use of electronic signatures, electronic contracts and electronic records by providing legal certainty for these instruments when signatories comply with its standards.

The Act broadly defines Electronic Signatures 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 is intentionally broad and technologically neutral to allow development of many types of technology and methods for signing electronically, while maintaining legal compliance.

Most American states have adopted another body of legislation called UETA (Uniform Electronic Transactions Act), which strives to make interstate commerce smooth on a national level. These federal initiatives are intended to bring a common understanding to electronic commerce, and have provisions that can pre-empt state laws which are not consistent with them. In addition, this legislation has preempted inconsistent State laws that were technology centric around PKI-specific 'digital signature' requirements.

As of May 2004, every state has legislation pertaining to electronic signatures (as opposed to "digital signatures" that are cryptographically based). Most have adopted the Federal UETA process, while others have adopted similar laws. By definition, an electronic signature can be just about anything produced by electronic means (e.g., a symbol, result, or consequence), which has been created electronically in order to demonstrate a party's intent to sign an electronic record.

Specific examples of electronic signing include entering a password or personal identification number (PIN), typing a name where indicated (or prompted) via computer keypad, responding to telephone keypad agreements (e.g., "press 3 to agree or 5 to hear this menu again"), responding to click

agreements, or even responding to an email thread—all can constitute an electronic signature. In several cases, courts have upheld server logs as evidence of contract agreement.

This new legislation effectively solves the "signed writing" problem, by establishing provisions that make electronic communication and contracts equivalent to their paper cousins:

- "Electronic Signature" is defined as an 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.
- "Electronic Record" means a created record generated, sent, communicated, received, or stored by electronic means.
- 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.
- If a law requires a signature, an electronic signature satisfies the law.

Are There Exceptions to ESIGN and UETA?

ESIGN and UETA define several contracts that are not covered by the legislation. This is not to say they are invalid as electronic transactions, they are simply not part of the ESIGN legislation. This list includes:

- Wills, codicils or testamentary trusts.
- UCC (Uniform Commercial Code) transactions (other than Article 2 and Article 2A transactions) generally are excluded, in the UETA (and NCUETA as per N.C.G.S. section 66-313(b)(2)), but in appropriate instances the UCC already provides or will provide for electronic treatment.
- Any notice of cancellation or termination of utility service or any notice of default, acceleration, repossession, foreclosure or eviction (or the Right to Cure) under a credit agreement secured by or a lease of a "private residence for an individual."

Key Factors for Enforceable E-Signatures

Intent

Intent is an important aspect of the e-signature process because it provides the legal "context" for enforceability. If the signer can claim to have "not understood" that they were actually signing a document, they may be able to mount a successful legal defense. With electronic signatures, the ability to establish intent can be of particular importance and can pose special challenges because the signing process does not take place within a structured physical setting (e.g. in a face-to-face meeting). Therefore the e-signature process should always provide a "structured online setting" that takes the signer through a series of steps, which make it clear that they are signing a legal document and confirms intent through overt actions like clicking a button or selecting a checkbox on a web page with a computer mouse.

Establishing Proof of Identity

Establishing proof of identity of the parties to the contract is a critical aspect of the signature process. In an online setting, this can be especially challenging because the parties do not "see each other" during the signing process and there is the risk that someone other than the intended signer(s) could be on the other end of the electronic transaction. Therefore, the e-signature system must include mechanisms for assuring that the person who completes the e-signing process is actually the intended party to the contract. This needs to be accomplished in a manner that firmly establishes proof of identity but also avoids imposing mechanisms that are too cumbersome or complex for most signers (such as requiring PKI digital certificates).

In addition, the system should provide the sender with multiple levels of authentication in order to allow tailoring of the proof of identity methods to fit their specific business requirements. Proof issues associated with electronic contracting present some challenging questions without a system to manage the contracting process. Anyone engaging in electronic contracting will need to make a careful risk/benefit determination around questions of proof.

A party to an electronic contract may have to go before a judge and show (a) that there was, in fact, a contract formed—i.e., there was an offer, and acceptance, and consideration; (b) what the substance of the contract was; and (c) who the contracting parties were. In general, identifying people and

notifying them via their email addresses is a reasonable mechanism for most transactions, since every email address is unique across all global boundaries.

Non-repudiation

Non-repudiation is an important concept when it comes to signing any legal documents. When we sign an agreement we seek to have that agreement be "non-repudiable' or done in such a way as to make it impossible for someone to deny they signed for one reason or another. Attempted repudiation of facts around the signing a contract can include:

- Repudiation of Content—"Someone made changes without agreement."
- Repudiation of Signer—"I did not sign that *or* that is not my signature"
- Repudiation of Change—"Somebody changed the document after I signed."
- Repudiation of Date—"I signed that before or after the indicated date."
- Repudiation of Intent—"I did not see that part of the contract!"

Now, having identified the pitfalls of any contracting process, here are the key points of how a credible electronic signature process addresses solves them.

The process must capture intent of the parties in a way that eliminates the possibility of e-signing a contract by mistake.

The process must enable the sending party to be certain that the contract is being received and signed by the person for whom it is intended.

The process must make repudiation of the contract impossible.

In summary, a robust e-signature process needs to provide a strong audit trail that captures the content of the document and intent of the signer, eliminates the risk of subsequent changes, and then creates an indisputable association between the contract, the date signed, and the signing parties.

Electronic Signature Removes Uncertainty and Inefficiency from the Contracting Process

Getting a wet signature via mail or fax is time and labour intensive and subject to error at any stage of a multi-part process. Sometimes the mail or courier envelope got lost or delayed. Sometimes the fax was unable to

transmit or was not legible. Traditional contract exchange and signing processes take valuable time and have an extra layer of work involved in maintaining storage of an executed contract after the fact. Datawitness collapses the sending, signing and storage process into one inclusive online application.

New electronic signature laws allow a purely electronic process for delivery of documents for signature. Datawitness uses a legally tested click wrap process that includes all steps required for binding electronic signature capture that will stand up in court.

The Datawitness SignOff™ process for e-signature is simple enough to present no technological hurdle to users, yet adheres to the legislation reviewed above in order to obtain a legally binding signature. Sending a contract via Signoff™ is as intuitive and user-friendly as sending email. Contract recipients can sign easily with just a click of a mouse.

All contracts flowing through the Datawitness system are authenticated for content and witnessed by Datawitness acting on your behalf as a trusted third party. Delivery of the contract to recipients is monitored so that the sender knows the status of a sent contract. Upon the recipient countersigning the contract, the sender is sent an email notice of the act of acceptance. Since each step is monitored, recorded and witnessed by a third party, the parties to a contract have the best evidence possible of online execution of agreements.

Take Comfort in 3rd Party Witnessed Proof

Have Datawitness present while you send a contract, or other type of form, for electronic signature. Datawitness SignOff™ acts as a third party witness to the content, timing, delivery, acceptance of a contract and protects you if a dispute arises over the agreement. A digital copy is accessible any time via the Internet, and a physical copy is kept on up to 500 year Kodak microfilm, and stored in our secure storage facility. You can rely on Datawitnessed records in court.

Datawitness authenticates your document and creates a unique digital fingerprint for each document you archive.. The fingerprint establishes proof of your document's authenticity. If the fingerprints of your archived document and the document you are comparing match, the documents are legally considered identical and guaranteed unaltered.

Sending a Contract Automatically Begins the Archiving Process

Datawitness' online filing, monitoring and retrieval system starts when you create and send a contract. SignOff™ s creates an authentic copy of each sent contract for online and off-site storage. The process continues as the contract is received and viewed by a recipient. SignOff™ captures the actions of the recipient up to and including electronic signature.

Benefits of Using Datawitness SignOff™

- Obtain signatures faster so you get more done in less time.
- Send and monitor multi-party signature requirements with ease.
- Send contracts from your computer in minutes and reduce printing and handling time.
- Archive contracts as part of the process and eliminate storage time and space.
- Reduce paper use and the direct costs of paper.
- Reduce the costs of moving paper by courier, post or fax.
- No software to install or purchase.
- Legally binding.
- Third party witnessing protects you.
- Best evidence tool for online agreements.
- Automatic archiving eliminates storage overhead.

SignOff™ is an online service that allows users to send contracts and receive signatures. SignOff™ witnesses the exchange to make a legally binding transaction.

To begin sending contracts quickly and securely and obtain legally binding electronic signatures in a fraction of the time required by traditional paper-based method, please call 1-866-273-6898 (North America) / 1-604-273-8894 (International) or email sales@datawitness.com.

Datawitness is a Canadian company based in Vancouver, B.C. Datawitness has a proprietary, web-based service that provides online services for signing, witnessing and archiving of vital records and important documents.

Datawitness overcomes the limitations of long term records archiving surrounding the authenticity and integrity of electronic documents; the repudiation of electronic agreements; the repudiation of electronic communications; email loss; intentional deletion; accusations of tampering; the retention of electronic files for compliance, audits, regulations; and the shelf life of digitally stored files.