
e Matters

A 6-POINT FRAMEWORK



Locke

Lord^{LLP}

BUSINESS
TECHNOLOGY
GROUP

Companies considering adopting an electronic signature process may be overwhelmed by the legal, regulatory, litigation, technological and other practical risks associated with an e-sign process. If so, the insights Locke Lord can provide may help. We have helped a number of clients design and implement effective electronic signature processes, from voice signatures to clicking "I Agree" on web sites to signing a hand held device. By tapping into Locke Lord's experience, our clients have confidently designed and implemented effective electronic signature processes.

Understanding the related technology and the regulatory environment is important. Designing an effective electronic signature and e-delivery process is, however, more about understanding workflow, and less about particular technologies.

e-Signature and e-Delivery Processes

Companies continue to search for ways to complete transactions with customers and suppliers faster and cheaper. The laws in every state recognize the use of electronic signatures, including for most consumer transactions. As such, more and more companies are looking for ways to supplement existing channels with an e-process, which would use an electronic signature (either at a web site, using a personal computer or over the telephone) to initiate or complete transactions.

There are many facets in designing and implementing an effective e-process. Below is an overview of some of the basics of the laws in this area, followed by a framework to understanding and managing the risks associated with an e-process.

Electronic Signature Basics

Federal vs. State Law

ESIGN, the federal law, does not preempt a state's laws dealing with electronic signatures if that state has adopted the model Uniform Electronic Transactions Act ("UETA") as published in 1999 by the National Conference of Commissioners on Uniform State Laws. As of the date of this article, at least 46 states have adopted UETA in one form or another. Not all of those 46 states have adopted a pristine version of UETA, and therefore they may be preempted in whole or in part.

With limited exceptions, the differences between or among the state enactments of UETA and the federal ESIGN law are insignificant, as a practical matter, in designing and implementing an effective e-signature process. The most significant difference between UETA adopted by the states and the federal ESIGN law relates to the consumer disclosure requirements. Both laws permit consumer disclosures to be provided exclusively through electronic means, but the federal law requires specific conditions to be met, which are not contained in UETA and none of the states adopting UETA have yet to opt out of the consumer disclosure requirements in the federal ESIGN law. For this reason, if consumer disclosures are to be provided exclusively through electronic means, the requirements of the federal consumer disclosure provisions will need to be satisfied, as explained more below.

Other differences between ESIGN and the states' enactment of UETA will not, as a practical matter, be significant. Consequently, most companies may design a national electronic signature process, without

having to contend with significant state variations in the electronic signature process. This point can be particularly important for insurance companies.

Because of the similarity between ESIGN and the state enactments of UETA which are not otherwise preempted by ESIGN, references below to ESIGN apply equally to a given state's enactment of UETA, unless otherwise noted. If a state has adopted UETA but has amended its enactment of UETA beyond that permitted by ESIGN, that state's enactment will be preempted by ESIGN, at least with respect to such non-permitted variation.

Recognition of e-Signatures

ESIGN states that a signature may not be denied legal effect solely because it is in electronic form. ESIGN does not give preferential treatment to electronic signatures. Consequently, an electronic signature can be challenged for all the other reasons that a wet signature can be challenged, such as the incapacity of the person signing, mistake, fraud, duress, and forgery. ESIGN does not require anyone to use or accept an electronic signature or record.

What is an "electronic signature?"

Selecting the method of electronically signing a document or record is the relatively simple element of an effective e-signature process. Under ESIGN (or the applicable state law) an electronic signature can be as simple or complex as:

- Clicking "I Agree;"
- Saying into a recording device, "I Agree;"
- Digital signature using PKI technology;
- Using a peripheral device that records an image of one's signature; or
- Other ways using an electronic sound, symbol, or process attached to or logically associated with the document or record, which is executed or adopted by a person with the intent to sign.

Verifications and Acknowledgements

Verifications and acknowledgments required by law to be in writing, such as certain notices in financial transactions, may be provided and obtained in electronic form under ESIGN in certain circumstances. ESIGN essentially provides that if a law requires a disclosure to be provided by a certain method that includes acknowledgment of receipt, that disclosure may be given electronically if, and only if, the electronic method for providing that disclosure also includes a process or method for capturing electronically an acknowledgment.

e-Delivery and Statutorily-Required Disclosures

ESIGN expressly permits disclosures that are required by law to be provided to consumers "in writing" and to be provided exclusively through electronic means if certain conditions are met. These conditions include: (i) obtaining the consumer's consent to receive the disclosures electronically; (ii) providing certain disclosures to the consumer to evidence the consumer's consent to receive the required disclosure electronically; (iii) receiving the consumer's consent to obtain disclosures

electronically prior to when in the sales transaction the disclosure sought to be electronically delivered is required by statute to be given; and (iv) providing a mechanism for the consumer to later access the record of the disclosure that was the subject of the consumer's consent.

Failure to comply with the ESIGN disclosure requirements does not render void or voidable the underlying transaction (for example, the application for insurance or the insurance policy ultimately issued), but could subject the company to regulatory sanctions for failing to provide the required disclosures (such as the replacement notice) in accordance with applicable law. There may also be civil remedies available to consumers if the disclosures are deemed to have not been given effectively.

Understanding how ESIGN applies to consumer disclosures is one of the most difficult aspects of designing and implementing an effective electronic signature process. Satisfying these requirements in the call center context is particularly challenging.

e-Record Retention

ESIGN allows an archived electronic record to satisfy applicable statutory requirements that a contract or other document be retained "in writing," if the electronic record is maintained in a form capable of being retrieved by all parties for later reference. In addition, ESIGN recognizes that records of a transaction (whether completed electronically or not) may be archived exclusively through electronic means, but failure to archive the records in a way that allows the record to be accurately reproduced could result in the unenforceability of the agreement represented by the electronic record and regulatory sanctions for failing to maintain the proper records. (For more detailed information on electronic record retention, please see the Locke Lord publication, "Information Management and Privacy.")

Limited Exclusions

Neither ESIGN nor the state enactments of UETA recognize the validity of electronic signatures in the following areas:

- Creation and execution of wills, codicils, or testamentary trusts;
- State laws governing adoption, divorce, or other matters of family law;
- Uniform Commercial Code, as in effect in any State, other than sections 1-107 and 1-206 and Articles 2 and 2A;
- Court orders or notices, or official court documents required to be executed in connection with court proceedings;
- Any notice of: the cancellation or termination of utility services; default, acceleration, repossession, foreclosure, or eviction, or the right to cure, under a credit agreement secured by, or a rental agreement for, a primary residence of an individual; the cancellation or termination of health insurance or benefits or life insurance benefits (excluding annuities); or recall of a product, or material failure of a product, that risks endangering health or safety;
- Any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.

A 6-Point Framework

Clients ask us to help them understand the risks associated with designing and implementing an effective electronic signature and electronic delivery process, as well as help them find ways to mitigate such risks. We have developed a 6-point framework that helps focus the attention of, and a common set of reference points for, a multi-disciplinary team involving legal, compliance, IT, operations and risk management involved in designing and implementing the e-process. The 6-point approach examines a proposed electronic signature and electronic delivery process from the following perspectives:



1. Authentication Risk

This is the risk that the electronic signature obtained is from a forger, not from the actual person whose name is associated with the electronic signature. The risk is that a company relying on an applicant's electronic signature to be that of a given person seeks to enforce the document bearing the person's signature and the person claims, "That is not my signature!"

There are ways to authenticate the identify of a person. A popular method is to use a "shared secret," such as combination of questions that nobody other than the real person would know, social security number, mother's maiden name, date of birth, employee number, etc. There are firms that can authenticate a person on a real time basis as well, using the shared secret approach. Using biometrics such as finger print, voice print or retinal scan are other ways. For some transactions, authenticating the identify of the person can be done after the signature is obtained.



2. Repudiation Risk

This is the risk that a document bearing a person's signature is altered after the document is signed electronically and the person repudiates the contents of the document bearing his or her signature. The risk is that a company relying on an applicant's electronic signature seeks to enforce the terms of the signed document bearing the applicant's signature and the applicant claims, "Yes, that is my signature, but the terms and conditions of what I signed are different than that document!"

There are ways to mitigate the repudiation risk considerably. In fact, our experience is that the repudiation risk can be reduced below the repudiation risk associated with traditional methods. The simplest way to mitigate repudiation risk is to have each document electronically sealed immediately after it is signed, to prevent any alteration to the document without such change being visible. Storing the documents in secure environments also mitigates the repudiation risk.



3. Compliance Risk

This is the risk that the rules and regulations governing such a transaction, such as regulation requiring certain consumer disclosures to be provided by a certain stage in the transaction, are not satisfied. The risk is that the company is sanctioned by regulatory authorities or the other party to the transaction avoids its obligations.

There are ways to mitigate this risk as well. As with the repudiation risk, our experience is that with a little bit of logic imbedded in an e-process, compliance can be better than in the traditional process. For example, an e-process with logic that requires all the disclosures to be provided and

acknowledged by a consumer can prevent completion of the process without all required disclosures being provided to the applicant.



4. Admissibility Risk

This is the risk that an e-contract is not admissible into evidence when the company seeks to enforce it. The 2007 *Lorraine v. Markel* decision put both litigators and litigants on notice that simply offering electronic evidence without laying the proper foundation, can deem such evidence inadmissible, and thus an e-contracting business process unenforceable.

There are various ways to improve the likelihood of the admissibility of e-contracts: by using an exemplar business process to designing customized systems for the creation, storage and production of electronic information.



5. Adoption Risk

This is the risk that the e-process takes longer than the traditional process or is not as convenient as the traditional process and consequently, adoption of the process is slow. The risk is that a company invests considerable resources to design an e-process only to find that there is little use of the e-process. The best way to mitigate this risk is to field test a proposed e-process.



6. Relative Risk

There are authentication risks, repudiation risks and compliance risks with the traditional process of using wet ink and hard copy paper to complete transactions. Many companies have not examined such risks until they begin developing an e-process. For most electronic signature and e-delivery processes, the goal will be to have the transaction, on the whole, be no riskier than the current processes.

The Locke Lord 6-point approach above helps clients focus on understanding and managing the risk to a level acceptable to our clients. There are ways to reduce the risk in each area above to levels at or well below the level of risk associated with using traditional processes.

Why Locke Lord?

We have helped a number of clients successfully design and implement effective electronic signature processes, in particular in the insurance and financial services areas. We have worked with a number of electronic signature vendors and understand the role technology plays in an effective e-process.

Further, we have conducted two mock trial presentations involving real state court judges where the focus of each trial was the use of electronic signatures. Both mock trials illustrated the challenges of actually enforcing documents signed using electronic signatures. The Locke Lord Technology Transactions Group helps clients design, implement and execute tactics and strategies to navigate the rapidly changing eBusiness landscape, including all aspects of marketing, soliciting and completing business over the internet and via other electronic means. Our lawyers have diverse backgrounds to effectively and efficiently respond to all client needs. We can help you exploit strategic opportunities and to protect your interests because we have the experience to help you execute your objectives. We don't just help you compete, we help you win.

Electronic Signatures Representative Transactions

- Advised several insurance companies on the risks of obtaining voice signatures via call center distribution channels;
- Advised a national insurance company in designing and implementing an electronic signature process using a hand held device on which signatures are obtained, including acknowledgements of receipt of consumer disclosures;
- Advised reinsurers on the overall effectiveness of insurance policies completed using electronic signatures and e-delivery of certain disclosures;
- Advised a surplus lines carrier in drafting an insurance policy covering the risks of inadmissability of documents signed electronically;
- Worked with in-house legal and IT teams to develop electronic signature platform for major medical and Medicaid insurance products; and
- Advised electronic signature solution vendor during product development stages with respect to electronic signatures and electronic records legal compliance issues.

For more information, visit our website practice pages or contact **Greg Casamento** (gcasamento@lockelord.com) or **Pat Hatfield** (phatfield@lockelord.com), Co-Chairs of the Business Technology Group.

