

"Proper Management of Electronically Stored Information (ESI) Requires Collaboration of Technical and Legal Expertise"

Unfamiliarity with Electronic Statutes, Regulations & Court Rulings and Amendments to the Federal Rules of Civil Procedure poses increased Management Risk when Converting from Paper to Electronic Transactions

---

Frank Maguire, Vice President Business Planning & Development
RPost, Registered E-mail

Overview: Electronic liabilities abound in both private and public sectors and by allowing employees access to e-mail systems without proper rules and procedures put into place, the likelihood of costly e-mail disaster increases. Changing technology and the evolving legal and regulatory governance of electronically stored information, ESI compound the problem. Effective operating rules and policy controls require a cohesive team effort of not only IT and legal departments but also HR, Finance and Compliance in addressing ESI strategy / management initiatives to protect against successful challenges.

Unfortunately, the evolution of digital information and its underlying statutes is today probably the least understood area of law. Lack of knowledge is seldom an acceptable legal defense and so the information accumulated in this chapter is offered as a broad overview of source material and in no way is meant to serve as legal advice. The intent is to acquaint the reader with background and relevant reference material to assist in more detailed analyses of the complexities involved in managing ESI properly.

Background: Love them or hate them regulations are put into place to help implement the underlying statute from which their authority ensues. However, due to an excess of caution on the part of those involved with the drafting and passage of federal electronic law, the decision was made to forgo the mandate of implementing regulations for fear that they would be too long in coming and too confusing and therefore counterproductive to the goal of boosting e-commerce / communication. Also, this lack of a mandate for implementing rules was in line with the priority of the time to keep on-line regulation light in order to foster innovation. Instead, industry felt obliged to design best practices standards and procedures as detailed in a 2003 private initiative relating to the 2000 ESIGN statute whose passage proved to be somewhat obscure – "Standards and Procedures for Electronic Records and Signatures," www.spers.org[1]. These standards

---

[1] **ELECTRONIC RECORDS AND SIGNATURES -- CHALLENGE AND OPPORTUNITY**
New eCommerce laws make possible the widespread replacement of paper documents with electronic records. They also enable the broad use of electronic signatures. Many businesses have begun converting their operations to avail themselves of the enormous advantages offered by electronic records systems.

While the new eCommerce laws permit the use of electronic records and signatures, they also require that electronic systems and processes meet specific standards for:

and procedures were intended to fill the regulatory void with practical user instruction, but dissemination proved to be a daunting task and the public / legal knowledge of ESIGN provisions proved to be limited. Generally regulations provide a blueprint to follow while acquainting readers with the thrust of the underlying law, but in this instance there were none and federal electronic law was slow to take hold despite its many benefits. [Aside: it is likely that the dot.com explosion and the onset of a recession were additional impediments to the underlying goal of replacing piles of paper with efficient electronic counterparts which delayed further the full benefits of e-commerce law.]

The end result of this sequence of events has created an environment in which the general public and legal / tech specialists have yet to fully embrace the many efficiencies and cost-saving provisions of the e-commerce statutes in order to convert day-to-day paper operations to an electronic format without loosing any legal protections.

Education is the key and that is why it is critical that public and private enterprises develop collaborative initiatives whereby all in-house stake-holders come to the table to air their concerns when launching new electronic activities. For instance, it is likely that many licenses / permits can be issued electronically instead of in hard-copy but it is necessary for the attorneys to sing-off on the legal aspects of conveyance and the legal strength of the electronic document; tech specialists must design an efficient delivery system with proper record retention, etc.; and policy people must be convinced that the electronic version has the same strength and attributes of hard-copy should it be challenged subsequent to delivery. Management reaps the benefit of such a collaborative effort as manpower, cost and response times will all be reduced and so it is critical that the developmental team have management's buy-in on the front-side of such an initiative, but all too often such projects are not coordinated properly and eventually die of their own weight before the true benefits are realized. In the end it is the taxpayer / customer who really benefits anytime cumbersome paper transactions can be converted to electronic as long as both parties to the transaction are protected and agree to the process.

With that as a backdrop it is important that anyone looking to design new electronic delivery systems be acquainted with e-commerce laws, regulations, e-discovery

---

- Obtaining consent to use electronic records and signatures,
- Presentation of information,
- Execution of signatures and creation of agreements,
- Record retention,
- Printing, and
- Delivery.

Failure to meet those standards may impair the enforceability of electronic records. As a result, companies are being forced to invest significant time, effort and manpower in answering questions about how to handle the practical, routine aspects of electronic transactions. Much of this time and effort could be avoided if industry-wide standards for these elements of electronic transactions could be established.

To address this problem, industry leaders have undertaken a cross-industry initiative to establish commonly understood "rules of the road" available to all parties seeking to take advantage of the powers conferred by ESIGN and UETA. The product of this initiative is the Standards and Procedures for Electronic Records and Signatures ("SPeRS").

initiatives and some important recent court rulings in order to be aware of the "hot buttons" and specific requirements that need be addressed.

ESIGN and UETA: ESIGN, the federal Electronic Signatures in global and National Commerce Act and UETA, the state-enacted Uniform Electronic Transactions Act were drafted with the intent of ensuring that electronic transactions would be afforded the same validity and legality as paper transactions – to accommodate and promote the efficiencies of digital information.

The foundation upon which these two laws are based can be broken down to the following rules:

- A record or signature may not be denied legal effect or enforceability solely because it is in electronic form;
- A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation;
- If a law requires a record to be in writing, an electronic record satisfies the law; and
- If a law requires a signature, an electronic signature satisfies the law.[2]

These three building blocks are themselves built upon three defined terms: "record, electronic record and electronic signature." Both UETA and ESIGN define a "record" as information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. An "electronic record" is similarly defined as a record created, generated, sent, communicated, received, or stored by electronic means. As a result, any type of document, contract, or other record of information could meet the definition of an electronic record if it were created, used, or stored in a medium other than paper. An "electronic signature" is 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.

Also, the drafters of ESIGN and UETA in their desire to facilitate the development of technology were cautious and took an agnostic approach to avoid specific technology requirements for the creation of records, electronic contracts, electronic signatures, etc. [3] UETA was promulgated in 1999 by the National Conference of Commissioners on Uniform Laws (NCUSL) [see www.nccusl.org for a copy] with forty-six states and DC, Puerto Rico and the Virgin Islands having adopted it in some form. The US Congress became concerned about the slow pace of states adopting UETA, and for some states their substantial changes to UETA, and so it enacted on June 30, 2000 a uniform national standard for the treatment of electronic records and signatures, ESIGN. Note: ESIGN shares many of the same provisions of UETA, but adds special consent requirements for consumer disclosures. There is an exception to ESIGN preemptive authority "only if" a state statute, rule, or regulation does not specify procedures that require or accord greater legal status to specific technologies or technical specifications.[4]

---

[2] UETA § 7; ESIGN § 101(a)
[3] Prefatory Note UETA 15 U.S.C. § 7004
[4] 101 (a)(2)(A)(ii) of ESIGN, 15 U.S.C. § 7002 (a)(2)(A)(ii)

While most of the Uniform Commercial Code other than Article 2 and 2A is excluded from coverage under both UETA and ESIGN, the UCC Articles governing funds transfers, letters of credit, security interests in personal property and securities all permit the use of electronic records and signatures for most purposes, according to their own terms. Consequently, most types of commercial agreements and related documents may now be delivered and executed electronically.

Note: The issue of preemption or deferral arises because of the mix of statutory authority one encounters when conducting electronic business in a variety of states – federal law, ESIGN and state law: majority being the Uniform Electronic Transactions Act (UETA) and some states being non-UETA statutes or common law, e.g. NY Electronic Signatures and Records Act (ESRA.) In short, conducting business transactions electronically in many states can raise the question of whether ESIGN preempts or defers to UETA and other state law.

Special Rules for Electronic Records (SPeRS Handbook 4/15/03 pg 3):

While ESIGN and UETA set no special standards for the use of electronic signatures, they do have a number of special rules for electronic records that are intended to substitute for certain types of writings. These rules include:

- *If a person is required by law to provide or deliver information in writing to another person, en electronic record only satisfies that requirement if the recipient may keep copy of the record for later reference and review. If the sender deliberately inhibits the recipient's ability to print or store the record, then the record doesn't satisfy the legal requirement.*
- *If a law or regulation requires that a record be retained, an electronic record satisfies that requirement only if it is accurate and remains accessible for later reference. The UETA does not say for how long it must be retained or to whom it must remain accessible. ESIGN provides that the record must be accessible to all people entitled by law to access for the retention period prescribed by law. Neither statute requires that the electronic record necessarily be accessible in a particular place – the parties entitled to access can, by agreement, establish a storage location.*
- *If a particular writing is required by law to be displayed in a particular format, the UETA does not change that requirement. For example, if a law requires a notice to be printed in at least 12-point type and a boldface font, that requirement remains in place under the UETA. If the law requires two elements of a document to be placed in a particular physical relationship to each other or some other part of the document, that requirement is not changed by the UETA. For example, if the law requires a disclosure to be displayed just above a contacting party's signature, that rule must be observed within the electronic record.*
- *If a law expressly requires a writing to be delivered by US mail for by hand delivery, the UETA does not change those delivery rules.*[5]

[5] UETA §§ 8 and 12(a); ESIGN §§ 101(d) and (e)

Generally speaking, these rules are not variable by agreement under either ESIGN or UETA; however, under UETA if the underlying statute requirement that information be delivered in writing, or by a particular delivery method, may be varied by agreement, then the requirement that an equivalent electronic record be capable of storage, or be delivered by the same method as a writing, may also be waived.[6]

Digital Information – Burden of Proof: Permitting electronic records to substitute for writings serves little purpose if the records are not admissible as evidence in the event of a dispute. The rule stated above is simple: A record or signature may not be excluded from evidence solely because it is in electronic form. An electronic record also qualifies as an original, even if that record is not the original form of the document, and satisfies statutory audit and record retention requirements. Beyond that, the ordinary rules of evidence will apply.

With this in mind, it is critical that private and public sector enterprises create and handle their electronic information properly so that there is proper accountability, authenticity is insured and records can be easily retained and retrieved. Federal regulatory requirements to prove certain characteristics of electronic information in order to prove authenticity have arisen in the fields of health-care, the financial services sector and in publicly traded companies. Consequently, business organizations must put electronic information policies in place to avoid regulatory non-compliance but more importantly to prevent electronic records from becoming compromised or worthless. Everyday electronic communication must be able to stand the test of evidentiary proof along with that of electronic records, transactions, etc. and it is the content not the technology that is critical during a challenge.

Federal Rules of Civil Procedure: The US Federal Courts in 2006 amended the Federal Rules of Civil Procedure with respect to e-discovery procedures. This action focused attention on the need for enterprises to take a pro-active approach in managing their electronically stored information, primarily e-mail, in order to successfully defend against a possible lawsuit. The Civil Procedure amendments were to clarify the following:

- ESI, including all e-mail messages and attachments, is discoverable and may be used as evidence in litigation – for or against an organization.
- During discovery, business record e-mail and all ESI related to current, or potential litigation, must be retained, stored and produced timely and in a legally compliant manner.
- Stored ESI can be purged if it is not relevant to ongoing litigation.
- Once litigation has commenced, back-up tapes cannot be written-over as this would be deemed to be illegal destruction of ESI.
- In order to be accepted as evidence, e-mail must be shown to have been recorded, preserved and retrieved in a tamperproof manner that is trustworthy and does not affect the authenticity of the original e-mail.

[6] UETA § 8(d)

While ESI / e-discovery issues have received much more attention in the past year from legal departments, the *Second Annual ESI Trends Report* issued by Kroll Ontrack, world leader in legal technologies found that "…both in the US and UK survey respondents are increasingly looking to IT departments to shoulder some of the ESI burden in policy development and enforcement. These finding reiterate that ESI management is no simple task and a true partnership with IT is required to make one's policy a success."

Key Court Decisions that impact ESI Management Concerns:

1. *Lorraine v. Markel American Insurance Company,* 2007 WL 1300739 (DMd May 4, 2007) by US Magistrate Judge Paul W. Gram. If you are to read only one recent court decision relating to admissibility of e-mails in evidence, etc. you should make it this one. Judge Grimm not only speaks to his instant opinion on the care needed in introducing electronic information into evidence under the Federal Rules of Evidence, but he goes on to create a basic primer dealing with some of the technology and document management issues raised by those requirements, such as hash values and other indicia of authenticity, metadata and collection techniques. He points out that a great deal had been written about rules regarding discovery of ESI, but little had been done to focus attention on "what is required to insure that ESI obtained during discovery is admissible into evidence at trial, or whether it constitutes 'such facts as would be admissible in evidence' for use in summary judgment practice."

   This landmark case speaks to some of the major shortcomings of standard e-mail. In this case, all of the printed e-mail evidence was discarded by the judge because neither party could authenticate the e-mail content or the transmission of electronic record data of the disputed e-mail message. Ultimately, the cost involved to the litigants may not have been significant, but the case highlights what is occurring regularly and quietly, often with far greater costs, behind closed doors in confidential binding arbitration.

   Judge Grimm's opinion should be read by those involved in designing and implementing processes for the treatment of ESI in general, e-contracting in particular and overall management systems with an eye on document creation, storage and retrieval, search capabilities, access rules, reproduction and admissibility. This opinion also points out that while neither ESIGN nor UETA afford greater strength to e-contracts and electronic signatures, all other rules that apply to wet signatures and hard-copy contracts, including rules of evidence, apply equally to e-records and e-contracts.

2. *Long v. Time Insurance Co.,* 572 F. Supp.2d 907, 2008 US Dist., LEXIS 79212. The court held in favor of the insurer on its motion for summary judgment based on the insured's false answer to a medical question on the application. The case speaks to the strength of an electronic signature and

should give some comfort to those looking to design e-contracting type solutions or other business processes.

3. *Aguilar v. Immigration & Customs Enforcement Div. of the US Dept. of Homeland Security,* 2008 WL 5062700 (S.D.N.Y. Nov. 21 2008). This US District Court issued a definitive ruling explaining that the US Federal Rules of Civil Procedure require that metadata associated with e-mails and electronic files be preserved, maintained and produced in the course of legal discovery. This case underscores the importance of preserving ESI and its associated metadata in order to avoid significant legal risk for not collecting and maintaining such digital evidence.

4. *EPCO Carbondioxide Products, Inc. v. JP Morgan Chase Bank, NA,* 2005 US Dist. LEXIS 43707 (W.D. La. June 6, 2005), rev'd and remanded 467 F.3d 466 (5th Cir. October 6, 2006). This decision is important as the 5th Circuit noted that UETA "allows an electronic signature to satisfy the signature requirements for most legal documents….(and) applies only to transactions between parties who have 'agreed to conduct transactions by electronic means.'" This is an important decision to review if one is proceeding with an e-contracting system.

5. *Bell v. Hollywood Entm't Corp.,* 2006 Ohio App. LEXIS 3950 (Aug. 3, 2006). Bell sued Hollywood for hostile work environment, sexual harassment and civil battery. In the employment application process, Bell completed her application electronically and in so doing acknowledged an arbitration clause. Because the electronic application process was shown to be handled correctly with the Plaintiff having selected the "yes" box in agreeing to take all disputes to arbitration, the court found that "Federal and Ohio law both authorize the use of electronic signatures and deem such signatures binding."

6. *Stevens v. Publicis,* 854 NYS 2d 690 (App. Div. 2008). The Court denied summary judgment to Stevens who was attempting to have enforced the original terms of his employment agreement, which had been amended by both parties in a series of e-mails containing typed signatures of both parties. The Court held that the typed name of the employing company's CEO at the end of the e-mail and Plaintiff's response, containing his typed name at the end of the e-mal, constituted "signed writings" and satisfied § 13(d) of Plaintiff's employment agreement, which required any modification be signed by both parties.

7. *State of New York v. Patanian,* 2008 NY Misc. LEXIS 2668. Electronically prepared traffic ticket with the police officer's pre-printed signature was deemed valid. The Court referenced ESIGN in finding that the officer's electronic signature had the "same validity and effect as one handwritten."

8. *Poly USA, Inc. v. Trex Co., Inc.,* W.D. Va. No. %:05 – CV-0031 (March 1, 2006). This decision clarifies that an e-mail sent by means of an office account does not automatically confer an electronic signature. The District Court found that "the use of a [Defendant's] Trex e-mail account to send an e-mail does not necessarily constitute and electronic signature under 15 U.S.C. § 7006 and, moreover, that Trex did not intend to electronically sign the e-mailed document by sending it from a Trex e-mail account" and therefore the document in question was not binding.

9. *JSO Assoc., Inc. V. Price,* 2008 NY Misc. LEXIS 2227 (Nassau Co. 2008). This case involved the question of whether Defendant was liable for a broker's commission to Plaintiff despite the fact that a memorandum included within the e-mail exchange appeared to be unsigned. The Defendant's name appeared in the e-mail address at the top of the e-mail but the e-mail itself was unsigned. The issue arose as to whether the statute of frauds had been satisfied since that statute required "a writing at the end of the memorandum." The Court pointed out that the law is still evolving as to how the statute of frauds will be satisfied for e-mail, etc. and therefore found that it must look for assurance as to "the source of the e-mail and authority of the person who sent it." This decision is quite significant as the Court held that "where there is no question as to the source and authenticity of an e-mail, the e-mail is 'signed' for purposes of the statute of frauds if Defendant's name clearly appears in the e-mail as the sender."

10. *Sims v. Stapleton Realty, Ltd.,* 2007 Wisc. App. LEXIS 741 (August 23, 2007). The Court of Appeals of Wisconsin found that the parties had in fact amended a paper listing contract by e-mail exchange that "constituted a written document under Wisconsin's Uniform Electronic Transactions Act (UETA)" and the e-mail amendments to the original listing contract withstood legal challenge after the fact.

Electronic Transactions – Value for Governmental Entities:

1. Reduced transaction costs
    - Reduce paper storage costs
    - Reduce processing time and internal mail costs
    - Reduce postage / overnight courier costs
    - Reduce labor / mail room costs
2. Reduced cost to taxpayers and enhanced service satisfaction
3. Increase taxpayer response times
4. Increase accountability and more efficient employee deployment
5. Decrease risk of failing to meet deadlines / response requirements

Electronic Transactions – Attributes:

1. Properly managed, e-mail records are admissible in court
2. With proper protections taken, e-mail record provides legal proof of delivery, content and official time stamps, and

3. Electronic signatures can be as effective as 'wet ink' signatures if properly executed.

Electronic Transactions – What is needed for Protection and increased Accountability: When reviewing software in the market, one should look for a core service that provides the sender with legal proof of delivery, content and official time stamp, including all attachments, where the recipient does not have to take compliant action for sender to be protected. Additional service features that may be considered include electronic signature, electronic contracting and end-to-end e-mail encryption. For instance a service could deliver a Registered E-mail message, with attachments and automatically return verifiable delivery evidence in the form of a Registered Receipt e-mail containing a digital snapshot of the content (message body and all attachments) and the official time the e-mail was sent and received by each designated recipient. An e-sign-off feature would incorporate a valid electronic signature of the recipient into the process where needed. As a means of providing accountable electronic communication, consider a technology that: a) does not store information on a central server; b) maintains the integrity of electronic communications and the security of the transmission using cryptography; c) provides the sender proof of delivery to the recipient; and d) provides an encrypted, tamper-proof record of the transaction that may include verifiable proof of both the delivery and acknowledgement or execution of any document.

Note: RPost Registered E-mail service provider is uniquely positioned to accomplish these tasks and many more.