ARTICLE:

THE ESSENTIAL ELEMENTS OF AN EFFECTIVE ELECTRONIC SIGNATURE PROCESS

By **Greg Casamento** and **Patrick Hatfield**[1]

Companies conducting business throughout the United States wanting to implement an electronic signature process (for customers, employees or suppliers) are provided little guidance from the electronic signature statutory schemes across the country. Those electronic signature laws, essentially two bodies of statutory law, provide that electronic signatures and electronic records may not be denied legal effect *solely* because they are in electronic form.[2] These laws do not give greater status to signatures or records in electronic form. Further, and more significantly, these laws do not describe any processes which, if followed, would result in enforceable contracts.

This article seeks to help those wanting to design and implement an effective electronic signature process by describing six perspectives from which a proposed electronic signature process should be evaluated. This six-point framework takes into account the legal and practical aspects beyond just the electronic signature laws, such as the rules of evidence. Examining the risks of an electronic signature process from these six perspectives allows one to match the mitigation measures for each risk with the level of risk acceptable for a given electronic signature process. For example, most will agree that an electronic signature process to buy a low priced book need not be as secure as an electronic signature process to buy an expensive item or for authorizing the disclosure of very sensitive information. This six-point framework helps to distinguish each risk to focus more clearly on the optimal way to mitigate each distinct risk.

The framework will help to answer the three fundamental questions that should be addressed for any proposed electronic signature process. This article includes an in-depth discussion of the essential elements that should be included in an electronic contracting process that will result in admissible evidence to enforce terms and conditions in records signed electronically in the United States of America, whether the electronic signature process is governed by the Federal electronic signature law or a particular state's enactment of the model electronic signature law.[3]

Critical risks and questions

Framework for evaluating the risks

Companies often approach their legal advisors for guidance on what steps an effective electronic signature process[4] should include. In seeking this guidance, companies have described a range of risks they associate with an electronic signature process. There are essentially five distinct risks for an electronic signature process, each of which should be examined relative to those same risks in dealing with paper and

[1] *The authors would also like to thank the editor for his valuable input in editing this article as well as Vita Zeltser, an associate of Locke Lord Bissell & Liddell LLP, for her assistance.*

[2] *The two bodies of laws are the federal act, the Electronic Signatures In Global and National Commerce Act, 15 U.S.C §70001 and following (referred to as ESIGN) and the various state enactments of the version of the Uniform Electronic Transactions Act, as published by the National Conference of Commissioners on Uniform State Laws (referred to as UETA). Forty seven states and the District of Columbia have enacted some version of UETA.*

[3] *There are significant differences between ESIGN the federal electronic signature law and the version of UETA adopted by forty-seven states and the District of Columbia. Except as expressly identified in this article, the differences are not significant for the topics described in this article. For example, UETA addresses when an electronic record is deemed to be sent by the sender and received by the addressee. The federal ESIGN law is silent on the topic.*

[4] *Throughout this article references to an 'electronic signature process' should be read to include the required disclosures of required terms, the delivery of the executed documents to the other party as well as the archival process for these records.*

manuscript signatures. These five risks and the benefit of examining each risk in context in this fashion comprise the Six-Point Framework identified below and discussed in more detail further below:

1. Authentication Risk – This is the risk that the signer[5] signing a record, accepting delivery of a record or providing a record is an imposter using a false identity; the records then being unenforceable by the user[6] against the person the user thought it was dealing with via electronic means.

2. Repudiation Risk – This is the risk that the signer claims that the electronic records that were signed were altered after they were signed, such that the person against whom enforcement is sought attempts to repudiate the actual terms and conditions in the signed electronic record.

3. Admissibility Risk – This is the risk that the other party to a transaction successfully challenges the admissibility of the necessary records, such as the signed contract, acknowledgment of receipt of certain disclosures, on the grounds of reliability.

4. Compliance Risk – This is the risk that the records signed or presented do not comply with other substantive laws, such as laws mandating certain content in documents to be presented or signed or do not comply with the basic requirements of ESIGN and UETA for delivery for such records.

5. Adoption Risk – This is the risk that in managing the risks above, an electronic signature process is so burdensome that the intended users are not satisfied with the process or find ways to avoid certain steps in the process, thereby undermining the process.

6. Relative Risk - In examining the risks above, users should evaluate the risk with a proposed electronic signature process *relative* to the corresponding risk in the process using paper and a manuscript signature, in the belief that an electronic signature process may not be risk free, but should not, on the whole, be any riskier than the paper and manuscript signature process, if feasible.

For the reasons explained below, it is possible to design an electronic signature process which is no riskier than, and in some areas, significantly less risky than, using paper and a manuscript signature. By examining the risks from these perspectives, it is easier to assess the particular risk and then determine the optimal means to mitigate the risk.

Critical questions

In reviewing a proposed electronic signature process, the following three fundamental questions should be considered:

a. Will the transactions executed using the proposed electronic signature process *be in compliance* with the applicable laws governing the use of electronic signatures and delivery of related electronic records, including the required consumer disclosures and consents, if any?

b. Will the records presented, signed, secured, archived and retrieved using the proposed electronic signature process be *admissible* in court (or arbitration) to enforce the terms and conditions in such records?

c. Will the terms and conditions in electronic documents signed using the proposed electronic signature process *be enforceable* against each signing party?

Subject to a subtle but important caveat, if each of the three questions above cannot be answered affirmatively, the electronic signature process should be re-examined, and appropriate changes made to the process. The transactions conducted through electronic means should be as compliant, generate records as admissible and result in terms as enforceable, as would be the case if those same records were completed on paper with manuscript signatures. In other words, aside from all the other applicable contract principles, such as capacity, fraud, duress, mistake, unconscionability, the records signed using the electronic signature process should be as enforceable as would be the case for those same records signed using a manuscript signature on paper.

[5] *The term 'signer' refers to the person, often a consumer, signing the electronic record, whether the record is a contract, application, consent, authorization or acknowledgement of receipt of terms.*

[6] *The term 'user' refers to the person, often a company, that has established the electronic signature process for enforceable and compliant transactions.*

Excluded areas

The focus of this article is on transactions between private parties, which include consumers. Excluded from the scope of this article are the following areas:

a. transactions dealing with the specific areas of the law expressly excluded from the federal ESIGN law and the state enactments of UETA, as described immediately below;

b. transactions dealing with any governmental agency where that agency is acting as a market participant;

c. execution of documents required by any governmental agencies which are not related to transactions between private parties, even if those documents are permitted to be filed with such an agency exclusively through electronic means, such as documents required to be filed with or maintained for inspection by the SEC or FDA;[7] or

d. records subject to any other law which specifies a particular method of verification or acknowledgment of receipt, such as requiring delivery by registered mail, return receipt required.

ESIGN and UETA do not apply to contracts and records that are governed by laws and regulations in only a few select areas.[8] Given the preemption provisions in ESIGN, the federal law, the states have limited authority to expand the scope of the areas excluded from ESIGN or the state enactment of UETA.[9]

Notwithstanding the foregoing exceptions, ESIGN (and UETA), when applied with other laws such as Revised article 9 of the Uniform Commercial Code, provide a mechanism for the use of electronic signatures and records in many of the most common business and consumer transactions, including contracts and records involving: (i) sales and leases of goods; (ii) insurance applications; (iii) mortgage loan documentation; and (iv) banking and investment transactions. ESIGN, the federal law, specifically applies to the business of insurance.[10] Given the similarity between ESIGN and UETA, insurance companies and other firms regulated under the state insurance codes, may adopt a uniform, national electronic signature process.

Legal analysis

ESIGN and UETA compared

For all purposes relevant to the analysis in this article, except as noted otherwise, the analysis under ESIGN (the federal statute), the relevant enacted version of UETA in 47 states and even under the non-UETA states, is essentially the same.[11] For those states that have adopted electronic signature laws governing interstate commerce inconsistent with ESIGN in areas relevant to the issues discussed in this article, ESIGN's broad preemption provisions will preempt such state laws.[12] For those states that have not adopted any electronic signature laws, ESIGN will govern as a result of its broad preemption provisions.[13]

The legal effect of electronic signatures

ESIGN recognizes that an electronic signature may be as legally effective as a signature applied on paper with a manuscript signature. ESIGN does not give electronic signatures a special status in the law. Rather, ESIGN states that a signature may not be denied legal effect *solely* because it is in electronic form. The foundational provision of ESIGN acknowledging electronic signatures provides, at § 101(a), the following:

(a) In General.--Notwithstanding any statute, regulation, or other rule of law (other than this title and title II), with respect to any transaction in or affecting interstate or foreign commerce-

(1) a signature, contract, or other record relating

[7] *This is not to say that the concepts described in this article do not apply to transactions with governmental agencies. Rather, this caveat is simply to alert the reader that certain governmental agencies may take the position that documents not related to transactions between private parties may not be within the scope of ESIGN and UETA.*

[8] *Excluded areas are: wills, codicils, and testamentary trusts; a state statute, regulation, or other rule of law governing adoption, divorce, or other matters of family law; the 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; notices for cancellation or termination of utility services (including water, heat, and power); notices of 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; notices of cancellation or termination of health insurance or benefits or life insurance benefits; recall notices of a product, or material failure of a product that risks endangering health or safety; and any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic and dangerous materials. ESIGN § 7003 (a), (b), UETA § 3.*

[9] *ESIGN § 102(a).*

[10] *ESIGN § 101(i).*

[11] *The states that have not adopted UETA are Illinois (adopted Electronic Commerce Security Act), New York (adopted Electronic Signatures and Records Act), and Washington (adopted Electronic Authentication Act).*

[12] *ESIGN § 102(a).*

[13] *ESIGN § 102(a).*

Another form of electronic signature is to say or select 'yes' over the telephone to accept terms and conditions contained in a writing acknowledged by the person so signing.

to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and

(2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

Thus, assuming ESIGN or UETA[14] applies to the transaction, each gives equal recognition to electronic signatures as given to manuscript signatures on paper.

Electronic signature defined

When a signature is created using a 'sound, symbol or process' that is 'attached to or logically associated with' a contract or other record by a signer with intent, such signature will be legally effective. For clarity, phrases such as 'legally effective' are used, rather than the statutory language of ESIGN, which states, 'not be denied legal effect solely because such signature is an electronic signature.' ESIGN § 106(5) defines an 'electronic signature' as:

> Electronic signature.--The term "electronic signature" means 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.

ESIGN § 106(4) defines 'electronic record' as:

> Electronic record.--The term "electronic record" means a contract or other record created, generated, sent, communicated, received, or stored by electronic means.

ESIGN § 106(9) defines 'record' as:

> Record.--The term "record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

Thus, an electronic signature may consist of an electronic sound or symbol, such as an individual saying 'I agree,' or typing 'I agree' or the person's name or following some other process, such as clicking 'I agree,' which is attached to or logically associated with information inscribed: (i) on a tangible medium, such as the tangible, hard copy of an authorization; or (ii) stored in an electronic medium retrievable in a perceivable form, such as the electronic record containing the identical information as contained in the tangible hard copy delivered to the consumer. Another form of electronic signature is to say or select 'yes' over the telephone to accept terms and conditions contained in a writing acknowledged by the person so signing.[15]

Users may select from a variety of ways to generate the signer's actual signature. The electronic signature process should clearly inform the signer that using such an electronic sound, symbol, or process is how the signer expresses his or her consent to sign such documents thereby evidencing his or her intent to be bound to such terms and conditions.

Evidence of the signer's intent to sign the record (which is required if the signer signs on paper with a manuscript signature) may be inferred (as it is with a manuscript signature on paper) from words close to the place of the signature where such words indicate in

[14] *ESIGN § 101(a); UETA § 7(a).*

[15] *See for example, Shroyer v. New Cingular Wireless Serv., Inc., 498 F.3d 976 (9th Cir. 2007) where an electronic signature process was recognized whereby terms and conditions contained in a printed booklet in a box in the consumer's possession for a consumer product are accepted by the consumer selecting 'yes' over the telephone. While the court recognized the electronic signature process, the terms of the contract were not enforced for reasons having nothing to do with the electronic signature process.*

clear and conspicuous terms the signer's intent to sign and be bound. For example, the text in the ESIGN Consent[16] could include the following text to explain the legal significance of the signer using the electronic signature process to create his or her electronic signature:

> By [describe method used to consent, e.g., selecting 'I AGREE'], you confirm that you have the computer hardware and software to obtain access to electronic records in the form that important disclosures will be provided to you in connection with [describe transactions], and you consent to receiving consumer disclosures related to [describe transaction] exclusively through electronic means.

Accordingly, pursuant to ESIGN and UETA, an electronic signature process where the significance of the process is clear may not be denied legal effect solely because it is in electronic form. Similarly, a document relating to such a transaction may not be denied legal effect, validity or enforceability solely because an electronic signature was used to sign such a document and subsequently stored as an electronic record, rather than in hard copy.

Consumer disclosures

On this topic of providing consumer disclosures exclusively by electronic means, there is a significant difference between the Federal ESIGN Act and UETA as enacted by many of the states. Both bodies of law (the federal ESIGN and the state enactments of UETA) permit consumer disclosures which are required by some other law to be given exclusively through electronic means, but the Federal ESIGN Act, and some, but not all, states which have enacted UETA, specify the process and the content for obtaining the consumer's consent to receive certain consumer disclosures exclusively through electronic means.[17]

ESIGN provides that, upon consent by the consumer, certain information relating to a transaction or transactions in or affecting interstate or foreign commerce, which is required by a statute, regulation, or rule of law (other than ESIGN) to be provided or made available to a consumer in writing (referred to as a Special Consumer Disclosure) may be delivered exclusively via electronic means, provided that the recipient of the Special Consumer Disclosure is first provided, and agrees to, the ESIGN Consent.[18] Whether a particular transaction requires a Special Consumer Disclosure, and how the ESIGN Consent is provided in connection with the required Special Consumer Disclosure, must be determined on a transaction-by-transaction basis. The user should identify which documents are Special Consumer Disclosures that require the need for the ESIGN Consent in the context of each type of transaction to be completed using the electronic signature process. The ESIGN provisions describing a Special Consumer Disclosure and the contents of the ESIGN Consent are set out in § 7001(c):

> If a statute, regulation, or other rule of law requires that information relating to a transaction or transactions in or affecting interstate or foreign commerce be provided or made available to a consumer *in writing*, the use of an electronic record to provide or make available (whichever is required) such information satisfies the requirement that such information be in writing if--
>
> (A) the consumer has affirmatively consented to such use and has not withdrawn such consent;
>
> (B) the consumer, prior to consenting, is provided with a clear and conspicuous statement--
>
> (i) informing the consumer of (I) any right or option of the consumer to have the record provided or made available on paper or in nonelectronic form, and (II) the right of the consumer to withdraw the consent to have the record provided or made available in an electronic form and of any conditions, consequences (which may include termination of the parties' relationship), or fees in the event of such withdrawal;
>
> (ii) informing the consumer of whether the consent applies (I) only to the particular

[16] *'ESIGN Consent' refers to the disclosure required by ESIGN to be provided to a signer who is a 'consumer' as defined by ESIGN, to which that signer must consent as a condition to the user providing one or more consumer disclosures required by law (referred to as a Special Consumer Disclosure) to that signer exclusively via electronic means, where such consent is given in a way that demonstrates the signer's ability to reasonably obtain access to information in electronic form the Special Consumer Disclosures will be provided.*

[17] *UETA §8(a) and ESIGN §7001(c). Providing Special Consumer Disclosures exclusively through electronic means is slightly complicated by the fact that a few states have included in their enactment of UETA provisions similar to those in the Federal ESIGN Act, as well as the fact that a federal law may require many Special Consumer Disclosures. For this reason, users are well advised to comply with the Federal ESIGN Act ESIGN Consent provisions discussed further below. See for example, Ala. Code 1975, § 8-1A-8(e).*

[18] *ESIGN §7001(c).*

transaction which gave rise to the obligation to provide the record, or (II) to identified categories of records that may be provided or made available during the course of the parties' relationship;

(iii) describing the procedures the consumer must use to withdraw consent as provided in clause (i) and to update information needed to contact the consumer electronically; and

(iv) informing the consumer (I) how, after the consent, the consumer may, upon request, obtain a paper copy of an electronic record, and (II) whether any fee will be charged for such copy;

(C) the consumer--

(i) prior to consenting, is provided with a statement of the hardware and software requirements for access to and retention of the electronic records; and

(ii) consents electronically, or confirms his or her consent electronically, in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent; and

(D) after the consent of a consumer in accordance with subparagraph (A), if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a subsequent electronic record that was the subject of the consent, the person providing the electronic record--

(i) provides the consumer with a statement of (I) the revised hardware and software requirements for access to and retention of the electronic records, and (II) the right to withdraw consent without the imposition of any fees for such withdrawal and without the imposition of any condition or consequence that was not disclosed under subparagraph (B)(i); and

(ii) again complies with subparagraph (C).

The signer's affirmative consent to the ESIGN Consent must exhibit the signer's ability to obtain access to information in the manner that the Special Consumer Disclosures will be provided. For example, if the required disclosure (a truth in lending disclosure for example) will be posted at a secure web site accessible only after the signer is given a unique access code, the signer should be given that unique access code during the ESIGN Consent process to confirm that the unique access code in fact allowed the signer to obtain access to the secure site where the Special Consumer Disclosures, such as the truth in lending statement, will be posted.

If the signer consents to receive such disclosures electronically but does not reasonably demonstrate his or her ability to obtain access to the information in the manner the Special Consumer Disclosures are provided, then the Special Consumer Disclosures are likely to be ineffective and therefore the basis for providing the required disclosures exclusively by electronic means could fail. Failure to comply with the ESIGN consumer disclosure requirements does not, however, render void or voidable the underlying transaction. ESIGN § 101(c)(3) provides:

> Effect of failure to obtain electronic consent or confirmation of consent.--The legal effectiveness, validity, or enforceability of any contract executed by a consumer shall not be denied solely because of the failure to obtain electronic consent or confirmation of consent by that consumer in accordance with paragraph (1)(C)(ii).

Failure to comply with the ESIGN consumer disclosure requirements could, however, subject the user to regulatory sanctions for failing to provide the required disclosures (such as the truth in lending notice in the example above) in accordance with applicable law. There may also be civil remedies available to signers if the disclosures are deemed to have not been given effectively. Not all notices or documents that users are required to provide to signers are Special Consumer Disclosures subject to the ESIGN disclosure requirements above. For such notices and documents which are *not* such Special Consumer Disclosures, the signer only needs to agree to receive such notices and documents exclusively via electronic means.

The user must first determine whether, for a given transaction, there are any Special Consumer Disclosures and, where there are, the electronic signature process:

(1) must present the appropriate ESIGN Consent to the signer, (2) should record that the signer consented to receive Special Consumer Disclosures exclusively through electronic means in a way that reasonably demonstrates the ability of the signer to obtain access to information in the electronic format the actual Special Consumer Disclosures will be provided or made available to the signer, and (3) for the Special Consumer Disclosures, provide or make available to the signer such disclosures in that same format. Taking these actions would allow the user to provide Special Consumer Disclosures in accordance with the requirements of ESIGN.

Use of an electronic process to complete transactions requiring Special Consumer Disclosures, or other documents containing mandated terms such as pre-approved forms, can actually reduce the user's compliance risk, compared to the conventional approach of paper and manuscript signatures. An automated electronic signature process allows the user to specify each document which must be presented and signed, as an acknowledgment of receipt or otherwise, as a condition to completing the transaction. Further, for an automated electronic signature process, the user can specify each particular which field in a record, such as an application for insurance, which must be completed as a condition to completing the entire transaction (as well as the nature of the information completed in such field, such as state of residence in a state where the user's products are not available). Thus, the user may configure the electronic signature process to prevent incomplete or non-compliant transactions from being submitted to the user for review. This can significantly improve the user's ability to comply with the requirements for such regulated transactions, and reduce risk while at the same time improve the rate of successfully completed transactions.

Verifications and acknowledgements

Verifications and acknowledgments required by law are expressly permitted to be delivered in electronic form under ESIGN in certain circumstances. ESIGN § 101(c)(2)(B) provides:

> Verification or acknowledgment.--If a law that was enacted prior to this Act expressly requires a record to be provided or made available by a specified method that requires verification or acknowledgment of receipt, the record may be provided or made available electronically only if the method used provides verification or acknowledgment of receipt (whichever is required).

Thus, if a law requires a disclosure to be provided by a certain method, which requires acknowledgment of receipt, such as delivery by first class mail, with proof of delivery required, such verification or acknowledgment may be given electronically if, and only if, the electronic method for providing such verification or acknowledgment also provides verification or acknowledgment of receipt. For example, the electronic signature process should be configured so that the consumer, before reviewing the verification or acknowledgement, must confirm receipt.

Record retention – sufficiency of electronic records

There are two record retention issues addressed by ESIGN. The first relates to the requirement that, where a statute requires a contract or other document to be in writing, the electronic record may be denied legal effect if all the parties or persons cannot reproduce it for reference entitled to the contract. The relevant section of ESIGN § 101(e) provides:

> Accuracy and Ability To Retain Contracts and Other Records.-- Notwithstanding subsection (a), if a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be in writing, the legal effect, validity, or enforceability of an electronic record of such contract or other record may be denied if such electronic record is not in a form that is capable of being retained and accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record.

Thus, if a user is going to rely exclusively on the archived electronic record to satisfy the statutory requirement that a contract or other document be in writing, failure to maintain the record in a form capable of being retrieved by all parties for later reference, could jeopardize the enforceability of the transaction to which such record relates. Users may satisfy this requirement by making the electronic record available to the signer for the required period of time, or the user may send a copy of the document or documents, in hard copy or electronically, so the user is not relying on the signer's

ability to obtain access to the electronic record maintained by the user.

In contrast, the second record retention issue relates to the user satisfying statutory record retention obligations. The user may electronically store the record (whether that record was initially in tangible form and later converted to an electronic form or initially in electronic form) of a transaction and thereby satisfy the statutory record retention requirement, provided certain conditions are met. ESIGN, § 101(d) provides:

> Retention of Contracts and Records.--
>
> (1) Accuracy and accessibility.--If a statute, regulation, or other rule of law requires that a contract or other record relating to a transaction in or affecting interstate or foreign commerce be retained, that requirement is met by retaining an electronic record of the information in the contract or other record that--
>
> (A) accurately reflects the information set forth in the contract or other record; and
>
> (B) remains accessible to all persons who are entitled to access by statute, regulation, or rule of law, for the period required by such statute, regulation, or rule of law, in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise.
>
> (2) Exception.--A requirement to retain a contract or other record in accordance with paragraph (1) does not apply to any information whose sole purpose is to enable the contract or other record to be sent, communicated, or received.
>
> (3) Originals.--If a statute, regulation, or other rule of law requires a contract or other record relating to a transaction in or affecting interstate or foreign commerce to be provided, available, or retained in its original form, or provides consequences if the contract or other record is not provided, available, or retained in its original form, that statute, regulation, or rule of law is satisfied by an electronic record that complies with paragraph (1).

ESIGN permits a user to satisfy its record retention obligations relating to transactions by retaining documents exclusively through electronic means. These ESIGN record retention requirements do not affect the user's record retention practices, except for those records relating to transactions to be retained exclusively through electronic means. Thus, if the user is satisfying the record retention obligations imposed on it by other laws by storing hard copies, ESIGN will not impose additional obligations.

As noted above, ESIGN does permit the user to satisfy its record retention obligations under applicable laws by retaining only the electronic records if the requirements of Section 101(e) of ESIGN are met. Thus, if documents in the audit trail,[19] which are required by law to be retained, are retained exclusively in electronic media, and are available to the regulators having jurisdiction over the user and such electronic records are available as described in Section 101(e) of ESIGN, the user may not be required to print and retain hard copies of these documents.

Notarizations

Signatures to be notarized may be notarized using an electronic notary process, providing that all other requirements of the notary laws are satisfied. ESIGN § 101(g) provides:

> Notarization and Acknowledgment.--If a statute, regulation, or other rule of law requires a signature or record relating to a transaction in or affecting interstate or foreign commerce to be notarized, acknowledged, verified, or made under oath, that requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable statute, regulation, or rule of law, is attached to or logically associated with the signature or record.

As stated further above, with limited exceptions, signatures will not be denied legal effect solely because they are electronic. Thus, if a law requires a signature to be notarized, either or both the signature to be notarized and the signature of the notary may be electronic signatures. All the other requirements for notarizing signatures (such as the notary must witness

[1] *'Audit trail' is a collective reference to the records containing the processes and details involved in each significant step of a given transaction involving a user including, the process of each signer accessing, completing, executing and transmitting each document to be signed in connection with the transaction, the user's process for authenticating each signer of each document for that transaction and all documents executed or resulting from the process, all as cryptographically sealed.*

Having signatures notarized is another form of authentication of the identity of the signer.

the person sign the document) must be met.

The official commentary to relevant provision in UETA (which is consistent with the notary provision in ESIGN) explains more about satisfying the notary requirement:

> This section permits a notary public and other authorized officers to act electronically, effectively removing the stamp/seal requirements. However, the section does not eliminate any of the other requirements of notarial laws, and consistent with the entire thrust of this Act, simply allows the signing and information to be accomplished in an electronic medium.
>
> For example, Buyer wishes to send a notarized Real Estate Purchase Agreement to Seller via e-mail. The notary must appear in the room with the Buyer, satisfy him/herself as to the identity of the Buyer, and swear to that identification. All that activity must be reflected as part of the electronic Purchase Agreement and the notary's electronic signature must appear as a part of the electronic real estate purchase contract.[20]

While ESIGN and UETA permit the notary requirements to be satisfied exclusively through electronic means, this does not require notaries to use electronic signatures or obligate private third parties requiring notarized signatures to accept the electronic signature of the notary.

Risk analysis framework and mitigation

Different categories of transactions present different risk profiles. For example, a transaction where a consumer authorizes the release of highly sensitive health or financial information to the person signing the release, presents a much greater risk of forgery than does a transaction for the purchase of a low-priced book. Likewise, a transaction for a consumer to sign an authorization to release sensitive health or financial information to an insurance company for underwriting purposes presents, as a practical matter, a lower forgery risk than if the sensitive information were to be released to the person signing, because the forger has less opportunity to benefit from the disclosure to the third party than from the disclosure directly to the forger, and therefore there is less incentive for a forger in the first instance. Because of these differences, when designing an electronic signature process, one should critically review the risks from various perspectives. The framework below identifies the six perspectives.

Authentication risk

This is the risk that a signer is in fact not the person he or she claims to be. A user may authenticate the identity of each signer in various ways. The identity of each person to sign should be verified. Such verification steps may include confirmation of the identity of such person from a trusted source, such as a single sign-on process deployed by, or otherwise determined to be reliable by the user. Alternatively, the results from an identity verification process conducted by an independent third party can be used for this purpose, such as a consumer reporting agency or other trusted third party offering such services. A further method can be used, such as the answer to a shared secret question that the user determines adequately verifies the identity of the signer. Having signatures notarized is another form of authentication of the identity of the signer. If there are documents required to be notarized, the electronic signature process should allow the notary verifying another signer's signature to enter the notary's signature and other credentials, in accordance with applicable state notary laws.

The method and results used to authenticate each

[20] *UETA § 11, Official Commentary.*

signer should be included in the archived signing session, or audit trail, which should then securely archived and capable of being retrieved securely. Where the user opts not to include the authentication process in the audit trail, the user may need to have access to other reliable evidence to establish the actual identity of the person completing the transaction.

As a practical matter, users should also critically evaluate the likelihood of forgers, or even signers who seek to disavow a given transaction claiming that a forger signed the documents. Consider, for example, the authentication risk in the context of applications for automobile insurance. The question that needs addressing is the likelihood of a consumer seeking to recover a payment for a covered claim contesting that he or she did not sign the application documents (which would include certain elections and waivers of coverage). To claim that a forger signed the documents would result in there being no cover, albeit for a different reason. Furthermore, it might also be useful to assess what motive a person have to forge the signature of another person for insurance cover on the car of the person whose signature is forged.[21]

At least one court has addressed this risk.[22] In Kerr, the employer sought to enforce a mandatory arbitration provision against an employee. The question was whether the employee did in fact sign the electronic record agreeing to be bound to the mandatory arbitration provisions. The court held that in light of the employee's credible claims that she did not sign the record containing the mandatory arbitration provisions combined with the employer's opportunity to sign such record using the employee's credentials, the mandatory arbitration provisions would not be enforced against the employee. Had the employee's supervisor not had such ready access to the employee's user name and password to obtain access to the secure site where the record in question was presented for signature, the court may have reached a different conclusion.

Repudiation risk

This is the risk of a signer acknowledging that he or she signed a document, but claims that the electronic signature is attached to or logically associated with a document containing terms and conditions different than those in the document the signer signed. The risk is that the signer repudiates the terms and conditions in the document attached to or logically associated with his or her signature and thereby reduces the chance that the document will be admissible and, if admitted into evidence, that the tier of fact will be persuaded that the signer did not agree to be bound by all such terms and conditions.

The electronic signature process should deploy readily available technology that can reduce the repudiation risk far below the repudiation risk associated with paper documents and manuscript signatures. The electronic signature process should cryptographically seal each document upon execution of that document by each signer, thereby rendering such document unalterable without detection. Documents electronically sealed in this fashion are likely to pass the admissibility threshold (for which, see the discussion below) and once such documents are admitted into evidence, users are likely to have meaningful, persuasive evidence as to why such document could not have been alerted without detection.

Each encrypted document should be securely stored in such a way that it cannot be viewed without overcoming at least industry standard security safeguards applicable to the document in question. For each transaction, whether the transaction involves two or more parties, the electronic signature process should record the date and time of each significant step and the identity of the person taking each such step and each particular step taken by that party, where such record is part of the audit trail. The audit trail for each transaction should include each document presented and signed during a given transaction where each such document signed having been encrypted as described above. Relevant parts of the audit trail should also be encrypted using industry standard encryption technology to render those portions of the audit trail unalterable without detection.[23]

Admissibility risk

This is the risk that a court refuses to admit into evidence copies of electronic documents generated, presented, signed, secured, archived and retrieved by

[21] *Admittedly, there is fraud in the automobile insurance sector, some of which involves forgery. Distinguishing the types of fraud and when fraud occurs in this area is essential to determine the mitigation measures with the actual risk presented in a given scenario.*

[22] *Kerr v. Dillard, 2009 U.S. Dist. LEXIS 11792 (D. Kansas 2009).*

[23] *The reader should be aware of the long-term viability of digital signatures when archiving digital documents protected by a digital signature, for which, see Stefanie Fischer-Dieskau and Daniel Wilke 'Electronically signed documents: legal requirements and measures for their long-term conservation', Digital Evidence and Electronic Signature Law Review, 3 (2006) 40 – 44.*

the electronic signature process. As a preliminarily point, it is important to recognize that all of the rules of evidence and evidentiary foundations that apply to paper documents and manuscript signatures also apply to electronic documents signed electronically, stored electronically and retrieved electronically. The Federal Rules of Evidence, or their state equivalents, govern the admissibility of evidence and thus would govern the admissibility of a copy of a document presented, signed, secured, archived and retrieved by the electronic signature process.[24] The electronic signature process should be able to satisfy the admissibility standards in the Federal Rules of Evidence to prove the authenticity of a document retrieved if the electronic signature process creates a reliable record of the entire signature process, including:

(a) the terms and conditions presented to the signer with which the electronic signature will be logically associated;

(b) the specific act of the signer expressing his or her intent to be bound to those terms and conditions, as called for in those same terms and conditions; and

(c) the circumstances under which signatures were obtained.

This information all goes to establish the authenticity of the document (containing the terms and conditions) retrieved by the electronic signature process. The electronic signature process should enable users to securely archive and retrieve the documents in a way to show that the documents containing the signatures could not have been altered without detection. The electronic signature process should also enable the appropriate witness on behalf of the user to provide an affidavit or live testimony as to items (a) – (c) above. For the reasons described below, such copies of documents generated by the electronic signature process based on documents presented, signed, secured, archived and retrieved by the electronic signature process should be as admissible under the Federal Rules of Evidence as such documents containing the same terms and conditions generated, presented, signed in hard copy and manuscript signature, where such paper copy is secured, archived and retrieved using conventional archival and retrieval methods.[25]

Federal Rules of Evidence

The standard for the authentication of evidence under the Federal Rules of Evidence is contained in Rule 901, Requirement of Authentication or Identification, which provides that 'the requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.'[26] As stated throughout the case law regarding the admissibility of computer generated information, '"reliability must be the watchword" in determining the admissibility of computer generated evidence.'[27] The 'factors [must] effectively address a witness' familiarity with the type of evidence and the method used to create it, and appropriately require that the witness be acquainted with the technology involved in the computer program used to generate the evidence.'[28]

Certain subparts of Sections 901 and 902 of the Federal Rules of Evidence are particularly suited to address the admission of electronic signatures and records: Sections 901(b)(1), (3), (4) and (9), and 902(7) and (11). Rules 901(b)(1), (3), (4) and (9) require witness testimony to authenticate proffered evidence, while 902(7) and (11) allow for self-authentication.[29]

F.R.E. 901

A witness with direct knowledge, pursuant to F.R.E.

[24] *Many states have adopted rules of evidence that track the Federal Rules of Evidence (FRE). For purposes of this discussion, all cases cited are based on the FRE or state law that follows the FRE.*

[25] *This would require the user to identify who, by name and title, is qualified to testify (in person or via an affidavit) as to how each document was presented, signed, secured after signature to render it unalterable without detection, archived, retrieved and printed. This person will also testify as to the integrity and security of each system involved in creating, securing, archiving, retrieving and printing the document.*

[26] *Lorraine v. Markel American Insurance Company, 241 F.R.D. 534, 541-42 (D.Md 2007).*

[27] *State v. Swinton, 268 Conn. 781, 812 (CT. 2004) (applying the federal standard to a state case).*

[28] *State v. Swinton at 813, 814.*

[29] *Magistrate Judge Paul W. Grimm's opinion in Lorraine v. Markel American Insurance Company provides ones of the best analysis to date of the admissibility of electronic evidence, which broadly could include electronic signatures, 241 F.R.D. at 542; Brian W. Esler, ' Lorraine v Markel: unnecessarily raising the standard for admissibility of electronic evidence, Digital Evidence and Electronic Signature Law Review' , 4 (2007) 80 - 82. See also In Re Vee Vinhnee, 336 B.R. 437 (proponent failed properly to authenticate exhibits of electronically stored business records); United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000) (proponent failed to authenticate exhibits taken from an organization's website); St. Luke's Cataract and Laser Institute PA v. Sanderson, 2006 WL 1320242, at *3-4 (M.D. Fla. May 12, 2006) (excluding exhibits because affidavits used to authenticate exhibits showing content of web pages were factually inaccurate and affiants lacked personal knowledge of facts); Rambus v. Infineon Tech. A.G., 348 F. Supp. 2d 698 (E.D. Va. 2004) (proponent failed to authenticate computer generated business records); Wady v. Provident Life and Accident Ins. Co. of Am., 216 F. Supp. 2d 1060 (C.D. Cal. 2002) (sustaining an objection to affidavit of witness offered to authenticate exhibit that contained documents taken from defendant's website because affiant lacked personal knowledge); Indianapolis Minority Contractors Assoc. Inc. v. Wiley, 1998 WL 1988826, at *7 (S.D. Ind. May 13, 1998) (proponent of computer records failed to show that they were from a system capable of producing reliable and accurate results, and therefore, failed to authenticate them).'*

901(b)(1), or an expert witness with learned knowledge, pursuant to F.R.E. 901(b)(3), are certainly two fairly straightforward methods a user could use to admit hard copies of documents signed using the electronic signature process. F.R.E. 901(b)(4), which permits exhibits to be authenticated by appearance, contents, substance, internal patterns, or other distinctive characteristics 'is one of the most frequently used [rules] to authenticate [electronic signatures] and other electronic records.'[30] F.R.E. 901(b)(9), which authorizes authentication by '[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result', is 'one method of authentication that is particularly useful in authenticating electronic evidence stored in or generated by computers' and is frequently used as a litmus test for admissibility of computer-related information.[31] '[It] dictates that the inquiry into the basic foundational admissibility requires sufficient evidence to authenticate both the accuracy of the image and the reliability of the machine producing the image.'[32]

The electronic signature process should secure each document after it is signed, as discussed above relating to the risk of repudiation. This would also allow the user to meet the admissibility standards under the subsections in F.R.E. 901. The testimony of a witness with knowledge of the specific transaction will satisfy F.R.E. 901(b)(1), and a learned expert witness should suffice under F.R.E. 901(b)(3). A witness knowledgeable about the contents, substance and distinctive characteristics of the electronic signature process of creating, presenting, signing, securing, archiving and retrieving the documents in question should satisfy F.R.E. 901(b)(4), while testimony describing how the electronic signature process accomplishes the foregoing accurately should suffice under F.R.E. 901(b)(9).

In addition to the express language of F.R.E. 901(b)(9), Imwinkelried's Evidentiary *Foundations* provides an eleven-step process under the Rule for the admission of computer generated records.[33] Most of the testimony proffered under these eleven steps is a simple recitation of facts. More challenging is step four, which requires proof that the 'procedure has built-in safeguards to ensure accuracy and identify errors … regarding computer policy and system control procedures, including control of access to the database, control of access to the program, recording and logging changes, backup practices, and audit procedures to assure the continuing integrity of the records.'[34] In satisfying this requirement or making arguments for admissibility under 901(b)(4), the user would need to provide expert technical testimony as to the functionality and safeguards in the electronic signature process.

Witness testimony seeking the admission of signatures and documents from the electronic signature process pursuant to F.R.E. 901(b)(9) would, in all likelihood, need to include:

a. The manner in which the user's server or servers, as appropriate, are used to generate electronic signatures and documents;

b. The reliability of these servers;

c. Procedures for manual data entry and system controls; and

d. Safeguards to ensure accuracy and identify errors (that is, safeguards, access rules and other controls on the environment that govern the flow of information through its system), tamper resistant software, use of cryptographic technology, and that all of these meet or exceed industry standards.

Presumably, after a number of court decisions recognizing the safeguards of a particular electronic signature process, such as by selecting "yes" in a recorded interactive voice recognition process as in the *Shroyer* case or a clear and conspicuous online process as in the *Bell* case, parties to transactions will be more inclined to stipulate, and not disagree about the authenticity of electronic signatures created using a given electronic signature process. If this were to occur, the need for witness testimony to authenticate

[30] *Lorraine at 544.*
[31] *Lorraine at 549.*
[32] *Swinton, 268 Conn. at 811.*
[33] *Edward J. Imwinkelried, Evidentiary Foundations, (LexisNexis 6th ed. 2005) 58-59, and see Stephen Mason, Electronic Evidence: Disclosure, Discovery & Admissibility (LexisNexis Butterworths, 2007), 4.23 for further comments on Professor Imwinkelried's list: 1. The business uses a computer; 2. The computer is reliable; 3. The business has developed a procedure for inserting data into the computer; 4. The procedure has built-in safeguards to ensure accuracy and identify errors; 5. The business keeps the computer in a good state of repair; 6. The witness had the computer readout certain data; 7. The witness used the proper procedures to obtain the readout; 8. The computer was in working order at the time the witness obtained the readout; 9. The witness recognizes the exhibit as the readout; 10. The witness explains how he or she recognizes the readout; 11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.*
[34] *In re Vee Vinhnee at 447. Opposing parties often allege that computer records have been tampered with and thus lack authenticity. Such claims have been viewed as 'almost wild-eyed speculation…without some evidence to support such a scenario….' United States v. Whitaker, 127 F.3d 595, 602 (7th Cir. 1997).*

documents may not be required in those later cases.[35]

F.R.E. 902

Although in a major dispute, testimony may be necessary regarding the electronic signature process and the authenticity of its process as noted above, documents presented, signed, secured, archived and retrieved using the electronic signature process may also be admitted as self-authenticating documents under F.R.E. 902(7). Judge Grimm in his opinion in *Lorraine v. Markel*, stated, at 549, that: '[e]xtrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to the following:...(7) Trade inscriptions and the like. Inscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin.' 'Under Rule 902(7), labels or tags affixed in the course of business require no authentication. The electronic signature process should collect and record information showing the entire signature ceremony. The identification markers alone stored in the secure container may be sufficient to authenticate an *electronic record* and *electronic signature* under Rule 902(7).'[36]

F.R.E. 902(11) of the Federal Rules of Evidence is the other subsection that might be considered for authentication of documents presented, signed, secured, archived and retrieved using the electronic signature process' electronic signatures. As Judge Grimm noted at 552: 'Rule 902(11) also is extremely useful because it affords a means of authenticating business records under Rule 803(6), one of the most used hearsay exceptions, without the need for a witness to testify in person at trial.' The primary reason for seeking to authenticate electronically stored information using this rule is that it permits a written declaration by a custodian rather than oral testimony, which under most circumstances makes it preferable to F.R.E. 901(b)(4) or (b)(9). F.R.E. 902(11) addresses:

> Certified domestic records of regularly conducted activity. The original or a duplicate of a domestic record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written declaration of its custodian or other qualified person, in a manner complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority, certifying that the record-
>
> (A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;
>
> (B) was kept in the course of the regularly conducted activity; and
>
> (C) was made by the regularly conducted activity as a regular practice.

Rule 902(11) was designed to work in tandem with an amendment to Rule 803(6) to allow proponents of business records to qualify them for admittance with an affidavit or similar written statement rather than the live testimony of a qualified witness. In addition to the affidavit requirements, there is a notice requirement to afford opposing parties an opportunity to review the document and affidavit to challenge its authenticity.[37] Thus, assuming no challenge, F.R.E. 902(11) is one of the best ways to secure the admission into evidence of signatures and documents executed using an electronic signature process.

As explained above, critical in the analysis of admissibility and the overall enforceability of documents executed using a given electronic signature process, is the requirement of a secure method to archive and retrieve the documents so they cannot be altered after signature. In addition to the method or process, there must be a credible person called by the user who is suitably qualified to explain the process:

a. the documents submitted to enforce the transaction are true, accurate and complete hard copies of each document signed by each signer that accurately reflect what the signer was presented with in connection with each signer using the electronic signature process;

b. the electronic signature process generates a true, accurate and complete hard copy of the audit trail for each transaction; and

[35] *For example see, Shroyer v. New Cingular Wireless Serv., Inc., 498 F.3d 976 (9th Cir. 2007) and Bell v. Hollywood Entm' t Corp., 2006 Ohio App. LEXIS 3950 (2006).*

[36] *Lorraine at 549, quoting Weinstein's Federal Evidence § 900.07[3].*

[37] *Federal Rules of Evidence 902 (11) at 773 at footnote 4.*

The audit trail should record each step required to meet the regulatory requirements, such as the sequence and timing of presenting certain forms and the actual contents of records presented.

c. the documents submitted to enforce the transaction were generated from electronic records that were cryptographically sealed in such a way that each record, as accurately represented by such hard copies, could not have been altered without detection, in the absence of a person using supercomputing power to break the encryption method used, currently thought to require several years of such supercomputing power.

Users should consider who would be qualified, willing and able to testify on the above items in designing the electronic signature process.

Compliance risk

The electronic signature process should assure that:

a. Each document presented or signed by a signer complies with the legal requirements for the content, presentation, sequence and information to be obtained for each such document;

b. For Special Consumer Disclosures, the signer is provided the appropriate information to enable them to make the informed consent in a way that complies with the consumer disclosure requirements of ESIGN, where such Special Consumer Disclosure Requirements will be provided exclusively via electronic means;

c. Each document required to be presented and signed is in fact presented and signed as required by law governing the particular transaction, and

d. The significance of each step in the signature process (whether on an acknowledgement of receipt, unilateral consent, application for goods or services, or contract) is abundantly clear to each signer.

The audit trail should record each step required to meet the regulatory requirements, such as the sequence and timing of presenting certain forms and the actual contents of records presented. The electronic signature process with the audit trail containing reliable, admissible evidence that each step was taken using the required content, a user may reduce the compliance risk considerably lower that the risk in transactions using paper and manuscript signatures.

The courts have been presented with a variety of disputes where a person alleged to have electronically sign a record disputes having signed the record. Where the significance of the steps involved in signing a particular record was made adequately clear to the person challenging the enforceability, the courts have enforced the electronic signature process. Where the significance was not sufficiently clear to the challenger, the courts have not enforced the terms against the challenger.[38]

Adoption risk

The adoption risk refers to the risk that the electronic signature process, in an attempt to reduce the authentication, repudiation, compliance and admissibility risks, is overly burdensome, such that the intended signers do not use the process or find alternatives that undermine the overall effectiveness of the proposed electronic signature process. This risk can, and should be, managed by conducting a series of pilot tests before introducing the electronic signature process

[38] *For example, see Bell v. Hollywood Entm' t Corp., 2006 Ohio App. LEXIS 3950 (2006) where the court enforced a mandatory arbitration provision against an executive of the defendant employer. The court found that it was sufficiently clear to the executive what the consequences were of selecting 'yes' in the electronic signature process. See also Brueggemann v. NCOA Select, Inc., et al., No.08-80606, 2009 WL 1873651(S. D. Fla. June 29, 2009), where the court enforced an electronic signature comprised of the process of continuing to use the website where the significance of proceeding was made sufficiently clear to a consumer purchasing consumer goods. In contrast, see Campbell v. Gen. Dynamics Gov' t Sys. Corp., 407 F.3d 546 (1st Cir. 2005), where the court concluded that the significance of not objecting to the terms was not sufficiently clear. The court refused to enforce the mandatory arbitration terms against the employee.*

to potential signers for the user. By conducting tests, the user can obtain feedback from the signers and make the appropriate adjustments.

Relative risk

As noted throughout this article, the risks of a given electronic signature process should be considered relative to the risks associated with a paper and manuscript signature. This allows the user to better assess the risks inherent in the particular electronic process. It is often easy to configure the electronic signature process to reduce the risks considerably below the corresponding risks of using paper and a manuscript signature. For example, the electronic signature process can be configured to prevent a record from being signed by the signer if there are any blanks in the record and prevent any document relating to a transaction from being submitted to the user unless all the required steps, including execution of or acknowledgement of receipt of all Special Consumer Disclosures, are fulfilled and then once signed and securing documents from being altered without detection. This can significantly reduce the compliance risk below that for paper and manuscript signature.

Conclusion

The overall effectiveness of a given electronic signature process depends on how well the user determined the means to mitigate the risks for particular documents and records to be presented, signed and archived. The user who carefully considers the risks associated with the types of transactions to be processed can design and implement an electronic signature process that is no riskier than, and in most cases, less risky than the same transaction using paper and a manuscript signature. Doing so provides greater confidence that the electronic signature, when affixed within US, will be admitted into evidence in a US court.

From the court decisions to date, there appears to be a premium placed on making it very clear to the person against whom enforcement is sought, the significance of the act comprising the electronic signature. The clearer the significance to the person signing, the more likely enforcement of the electronic signature process. Enforcement of the electronic signature process will not, however, overcome terms and conditions otherwise unenforceable for reasons having nothing to do with the electronic signature process, such as unconscionable terms in mandatory arbitration agreements.

It is to be expected that as the significance of actions comprising the electronic signature are made clearer, persons aiming to avoid obligations in signed agreements will look for other ways to avoid liability, such as challenging the admissibility of the electronic records for various reasons. The framework described in this article should help companies critically evaluate those risks with the aim of determining what measures to implement that are appropriate within the risk assessment profile discussed in this article.

Greg Casamento and Pat Hatfield are both partners in Locke Lord Bissell & Liddell LLP, a national law firm with offices across the United States. Greg practices in the area of electronic commerce and related litigation matters, including e-discovery and e-admissibility. Pat practices in the electronic commerce, intellectual property and technology areas. The views expressed in this article are those of the authors and do not constitute legal advice regarding any particular set of facts, products or services.

PHatfield@lockelord.com
GCasamento@lockelord.com

http://www.lockelord.com/