New Strategic Analysis:
Guidelines for e-Signature and e-Delivery in the Insurance Business

In an effort to foster a better understanding of ESIGN (Electronic Signatures in Global and National Commerce Act) and UETA (Uniform Electronic Transactions Act) as they pertain to the insurance industry, ACORD engaged Locke Lord, LLC to write the following strategic analysis — *Guidelines for e-Signature and e-Delivery In the Insurance Business*

By fostering a greater understanding of the legal requirements for both electronic signatures and electronic delivery of documents, we believe that this Strategic Analysis will serve as a foundational document for insurers and producers with interests in these capabilities.

The analysis contains:

- A summary of the legal requirements of ESIGN and UETA*
- A list of the recommended best practices for implementing electronic signatures in insurance
- A glossary of common term definitions with respect to electronic signatures

Please note: the Strategic Analysis presented does not represent legal or other professional advice and is not a substitute for the advice of an attorney. If you require legal advice, you should seek the services of a qualified attorney.

*as summarized by Locke Lord, LLP

Two Blue Hill Plaza
3rd Floor
Pearl River, NY 10965-8529, USA
Tel: +1 845 620 1700 Fax: +1 845 620 3600

www.acord.org

London Underwriting Centre
Suite 1/3, 3 Minster Court
Mincing Lane, London EC3R 7DD, UK
Tel: +44 (0)20 7617 6400 Fax: +44 (0)20 7617 6401

Locke Lord LLP
Attorneys & Counselors

GUIDELINES FOR *e*-SIGNATURE AND *e*-DELIVERY IN THE INSURANCE BUSINESS

By: Gregory T. Casamento and Patrick J. Hatfield*

INTRODUCTION

ACORD asked us to summarize the legal requirements applicable to using electronic signatures, electronic records and electronic delivery in the business of insurance. Our goal is to help ACORD members and the larger insurance community to understand the legal requirements applicable to designing and implementing an effective and compliant electronic signature and delivery processes. The concepts in this paper apply to all lines of insurance, except where the context clearly indicates otherwise. In this paper we summarize the legal requirements as well as identify what we believe are some of the best practices in implementing and using electronic signatures, records and delivery in the insurance business.

TERMINOLOGY

People may assign different meanings to some of the key terms in this area. For example, a security professional may use "digital signature" to refer to a method for two devices to establish a secure, recognized connection, while a marketing professional may use "digital signature" to refer to how a consumer signs an application for insurance online. Both persons would be correct, from their perspective. To reduce confusion, at the end of this paper is a glossary of capitalized terms as those terms are used in this paper.

LEGAL REQUIREMENTS

The Basics

Both ESIGN and UETA give legal recognition for Electronic Signatures and Electronic Records to satisfy the "in writing" Legal Requirements for transactions and permit companies to satisfy statutory record retention requirements solely through the use of Electronic Records. These laws apply broadly to a wide range of transactions, including those involving a consumer and those between companies. Both ESIGN and UETA require each person's consent to conduct business electronically. There are, however, special rules for providing disclosures to consumers electronically, as discussed further below.

These laws also give legal recognition to the use of Electronic Records to satisfy the "in writing" Legal Requirements relating to consumer disclosures (more below on this topic). The "in writing" requirement for other documents used in the insurance business, such as applications, consents, acknowledgments, waivers and notices can be satisfied with Electronic Signatures and Electronic Records in the appropriate circumstances.

---

* Messrs. Casamento and Hatfield are both partners in the law firm of Locke Lord LLP (www.LockeLord.com). The authors express gratitude to Lloyd Chumbley and Marcia Berner, both of ACORD, for their leadership and comments on this paper. This paper is a summary of certain aspects of the applicable law and is not intended to be relied upon as legal advice.

Both ESIGN and UETA identify a number of categories of transactions or records, where electronic records will not necessarily be recognized. For example, both bodies of law expressly state that notices to terminate utility services may not be sent exclusively by electronic means. Most of these categories not covered by ESIGN or UETA do not relate to the business of insurance. There are two exceptions that may impact some lines of insurance.

One exception is that the legal recognition of Electronic Signatures and Electronic Records does not apply to documents relating to wills, codicils or testamentary trusts. This exception could be relevant in some estate planning techniques involving life insurance and testamentary trusts. The second possibly relevant exception is that notices of termination of health insurance or benefits of life insurance (excluding annuities) may not be given solely via e-delivery.

Interplay between Federal ESIGN and State Enactments of UETA

ESIGN became effective on October 1, 2000. That federal law recognizes the legality of Electronic Signatures, electronic delivery and electronic archival as methods for satisfying the requirements to have written signatures and records. ESIGN also expressly states that it applies to the business of insurance.

After ESIGN was enacted, it gave states reasons to enact, as a state law, the model version of UETA. For those states that have adopted the model version of UETA, the state law will govern. Under ESIGN, if a state imposes greater restrictions on the use of Electronic Signatures or Electronic Records (such as mandating a particular type of technology), that state's law is preempted, or overruled, by ESIGN, meaning that the provisions in ESIGN control, not that state's more restrictive law. For purposes of the topics covered in this paper, with one significant exception relating to consumer disclosures (discussed further below), the Legal Requirements under ESIGN and UETA are quite similar.

Because the two bodies of law are… quite similar… there is not the same level of state-specific provisions in the governing Electronic Signature laws, as the insurance industry is accustomed to seeing in other areas.

As of the date of this paper, Illinois, New York and Washington are the only states that have not enacted UETA. These three states' laws governing electronic signatures, records and delivery (whether in the state's insurance code or in separate electronic signature laws) will be preempted, or overruled, by ESIGN, to the extent the state's existing electronic signature laws conflict with ESIGN, at least for those transactions governed by ESIGN, which includes transactions in the business of insurance.

Thus, for purposes of determining the applicable Legal Requirements, one can look to the model UETA and ESIGN as a meaningful starting point. Because the two bodies of law are, as a practical matter, quite similar, and because of the preemption provisions in ESIGN, there is not the same level of state-specific provisions in the governing Electronic Signature laws, as the insurance industry is accustomed to seeing in other areas. There is, however, one exception relating to how consumer disclosures may be presented, as discussed further below.

e-Signatures and *e*-Records Blessed but not Elevated

Both ESIGN and UETA state that signatures and records which are required to be "in writing" may not be denied solely because they are electronic. These bodies of law give legal legitimacy to Electronic Signatures and Electronic Records, but do not give Electronic Signatures or Electronic Records any special status. All the other Legal Requirements of documents to be presented still govern. For example, where an insurance code requires an application for insurance to contain certain information, the electronic form of that application must contain that same information.[1]

Where a law requires a record to be provided or made available in a specified method that requires verification or confirmation of receipt, both ESIGN and UETA expressly state that an electronic record may be used, but only if the delivery method provides for such verification or confirmation of receipt, as required. Where a law requires a record to be signed in the presence of a notary, an Electronic Signature on an Electronic Record with that same content must still be notarized, which may be done electronically as well.

Electronic Delivery – Generally

Both ESIGN and UETA recognize that insurers and Producers may satisfy the delivery Legal Requirements by providing Electronic Records, but the required sequence of steps must still be met. For example, if an insurance code requires that a certain election be made by the consumer before the application is completed, the Electronic Record with that election would need to be made by that consumer **before** the application is completed. Legal Requirements specific to records that are "consumer disclosures" (such as those required by an insurance code) and which must be delivered "in writing" are discussed below.

Unrelated to the Electronic Signature laws but certainly related to the Legal Requirements for an Electronic Signature and electronic delivery process are privacy laws and data security laws. These laws require that the electronic transaction processes (taking applications, delivery of the insurance policy package, policyholder services transactions and other transactions involving sensitive information) be conducted securely, where, for example, sensitive health information, social security numbers and other sensitive data be transmitted through only secure channels.

Both ESIGN and UETA recognize that insurers and Producers may satisfy the delivery Legal Requirements by providing Electronic Records, but the required sequence of steps must still be met.

Electronic Delivery – Special Consumer Disclosures

One of the more difficult aspects in understanding the practical impact of these laws relates to consumer disclosures. The insurance codes contain a number of Legal Requirements to provide consumers with disclosures in writing. In life insurance, for example, the Producer or insurer may be required to provide a replacement notice in writing at the time the application is taken. In personal lines auto coverage, the Producer or insurer may be required to inform the consumer in writing of the availability of uninsured / underinsured motorist coverage, and obtain the consumer's signature or initials on that disclosure form. In this paper, we refer to this type of disclosure required by the insurance code to be given to a consumer in writing as a Special Consumer Disclosure. Of course, where a Special Consumer Disclosure or other type of form is

required to be signed by the consumer, an electronic signature process can satisfy those Legal Requirements.

Under both ESIGN and UETA, Special Consumer Disclosures may be provided solely via e-delivery. While both bodies of law permit consumer disclosures to be provided solely via e-delivery, ESIGN contains an additional **procedural** Legal Requirement not found in UETA[2] relating to how consumer disclosures are provided electronically. This procedural requirement is the Legal Requirement that after the consumer is informed of certain aspects of how information will be provided through electronic means, the consumer must reasonably demonstrate the ability to open an electronic record in the format that the Special Consumer Disclosures will be provided. The consumer must reasonably demonstrate the ability to open an electronic record in the format the Special Consumer Disclosure(s) will be sent before the Special Consumer Disclosure is delivered to the consumer. Thus, the Legal Requirement under ESIGN is that if an insurance code requires a Special Consumer Disclosure to be provided before the consumer signs the application for insurance, the consumer must (i) be informed of the required aspects of how the information will be provided electronically, (ii) the consumer must reasonably demonstrate the ability to open an electronic record in the way that Special Consumer Disclosure will be sent electronically and (iii) receive that Special Consumer Disclosure, all before the consumer signs the application for insurance.

Under both ESIGN and UETA, Special Consumer Disclosures may be provided solely via e-delivery.

The following 17 states have adopted UETA and in their enactments of UETA have included the ESIGN consumer disclosure provisions: AK[3], AL[4], CO[5], CT[6], GA[7], MD[8], MA[9], NH[10], NV[11], NC[12], NJ[13], OR[14]SC[15], TN[16] ,VT[17], WV[18] and WI[19]. Consequently, for these states, for consumer disclosures required by state law or by federal law, the consumer disclosure provisions and the method of consenting as described in ESIGN governs. As described above, the ESIGN Consent and delivery of the Special Consumer Disclosure steps must be completed at or before when the insurance code requires that Special Consumer Disclosure to be delivered. In other words, if the insurance code requires a Special Consumer Disclosure to be provided in writing before the application for insurance is signed, the ESIGN Consent requirements need to be completed and the consumer must be given the Special Consumer Disclosure before the consumer signs the application.

For the other thirty (30) states that have enacted a version of UETA but have not included in their enactment of UETA the special ESIGN consumer disclosure provisions, the consumer must still consent to receive disclosures electronically, instead of in writing. A consumer's consent to complete the transaction electronically is not enough to satisfy the Legal Requirement that the consumer must also consent to receive disclosures electronically. In these thirty (30) states, however, for consumer disclosures required by an insurance code, the Special Consumer Disclosure Legal Requirements (as described above) do not apply and the law is met simply by obtaining the consumer's consent.

Another Legal Requirement under both ESIGN and UETA relating to Special Consumer Disclosures is that the Electronic Record must be provided or made accessible to the consumer for later reference. This is particularly relevant when consumers use a Producer's computer to complete the application for insurance. If the Special Consumer Disclosure is displayed on the Producer's screen but not actually delivered to the consumer (at the consumer's personal email address, for example), or otherwise made accessible to the consumer (such as posting on a website readily accessible to the consumer or providing a paper copy at that time), the Producer

has not met the Legal Requirements.[20] Using email delivery, providing access to the documents on a secure website or other methods may be used to meet the access requirement. While the focus of this section of this paper is on Special Consumer Disclosures, the point in this paragraph applies to other records required to be provided, delivered or made accessible to consumers.

Voice Signatures and Special Consumer Disclosures

The Legal Requirements for a signature can be met with a voice signature under ESIGN and UETA. A voice signature (such as the person saying, "Yes, I agree to be bound to the terms of this application.") can satisfy the Electronic Signature Legal Requirements, as long as that voice signature is attached to or logically associated with a record containing the terms to which the person speaking those words intends to be bound. Obtaining a consumer's consent to receive Special Consumer Disclosures over the telephone presents a special challenge.

ESIGN expressly states that merely recording the reading of a Special Consumer Disclosure to the consumer does not satisfy the Legal Requirement that the consumer receive that Special Consumer Disclosure, even though there is an Electronic Record of the disclosure. This provision is one of the most often misunderstood provisions in ESIGN. To meet the Legal Requirements in these circumstances, the Electronic Record of the Special Consumer Disclosure read to the consumer would need to be provided or made available to the consumer at or before when the insurance code requires that Special Consumer Disclosure to be provided to the consumer. Alternatives for satisfying the Legal Requirements in this particular scenario involving voice signatures is beyond the space limitations of this paper.

Record Retention Requirements

Both ESIGN and UETA allow companies to satisfy their record retention Legal Requirements exclusively through the use of Electronic Records. For Electronic Records (imaged records, for example) to satisfy the Legal Requirements to retain records in writing for a specified period, a person must store the Electronic Records accurately and do so in a way that makes the records accessible to all persons (including regulators) who are entitled by law to access such records. For this reason, the Electronic Records must be securely archived, indexed, and capable of being retrieved on a timely basis. These provisions in ESIGN and UETA may be relevant to responding to market conduct exams when regulatory examiners may request, for example, copies of Special Consumer Disclosures provided to a given consumer, evidence that a given consumer consented to complete the application materials electronically or other records beyond Special Consumer Disclosures the company is required to retain under federal or state laws.

Authentication

Relying on Electronic Signatures is thought to have higher risk because the chance of forgery is greater, especially for transactions completed online. Companies therefore focus on effective methods to Authenticate (or verify) the actual identity of persons signing insurance documents using Electronic Signatures. There are various ways to mitigate this Authentication risk (the risk that the person signing is not in fact the person he or she claims to be). As a first step, companies should consider the likelihood and magnitude of harm of forgery on the particular documents to be signed using an Electronic Signature. (For example, what would a forger gain by signing.) Next, companies should consider the options for Authenticating the identity of each person signing those forms. The "shared secrets" method is frequently used to Authenticate persons. This method consists of asking questions a forger is not likely to know,

such as a combination of driver's license number, Social Security Number and other information only the real person is likely to know. Other methods of authenticating a person include using biometric information, such as finger prints or retinal scans.

The degree to which a company seeks to Authenticate the identity of each person signing the documents should match the likelihood of forgery and the level of harm that would be caused if a forger were to sign the document. For example, on forms to insure a vehicle, the risk of a forger insuring a vehicle of another person might be viewed as quite low and as such, the steps to Authenticate the identity of the person applying for that coverage might be few. Companies should match the Authentication steps according to the risk of forgery to the type of transaction.

The degree to which a company seeks to Authenticate… each person… should match the likelihood of forgery and the level of harm… if a forger were to sign the document.

Neither ESIGN nor UETA specify methods of Authentication. Nevertheless, we consider applying the *appropriate* level of Authentication as a Legal Requirement, not just Best Practices.

Repudiation

In the absence of a process to protect them, Electronic Records are generally easier to alter than are paper records. Further, one's original wet-ink signature cannot be extracted easily from a paper record and affixed to another original paper without it being apparent what happened. This is not necessarily so with Electronic Signatures on Electronic Records. For this reason, companies designing an Electronic Signature process should consider the risk that the other party to a transaction (generally, the person completing the application for insurance, changing insurance coverage, acknowledging receipt of a form, making an election or the host of other insurance documents a person signs) may Repudiate the contents of an Electronic Record containing that person's Electronic Signature.

The person seeking to Repudiate an Electronic Record containing his or her Electronic Signature would claim that the Electronic Record was altered after he or she signed it. Alternatively, that person may claim that his or her Electronic Signature was extracted from an Electronic Record signed and affixed to another Electronic Record that he or she did not sign.

To mitigate the risk relating to a person attempting to Repudiate an Electronic Record bearing that person's Electronic Signature, companies designing an Electronic Signature process should include an Audit Trail in their process and deploy a technology to apply a Tamper Seal to Electronic Records signed using an Electronic Signature. Neither ESIGN nor UETA require the use of Audit Trails or Tamper Seals. Audit Trails and Tamper Seals will improve the likelihood of Electronic Records with Electronic Signatures being admitted into court and will improve their persuasiveness to prove what the person actually signed. For this reason, we consider using Audit Trails and Tamper Seals as Legal Requirements, not just Best Practices.

Admissibility Requirements

Neither ESIGN nor UETA address the topic of how one may enforce the terms of an electronically signed record against the other party to that transaction. Rather, it is in the federal and state rules of evidence that one will find these Legal Requirements. The rules of evidence require certain information to be provided to admit electronically signed records into evidence.

Admitting an Electronic Record into evidence is critical if there is a dispute over the terms of the record. In particular, the company seeking to enforce terms and conditions in a record (such as a false statement in an application for life insurance or an election to waive uninsured motorist coverage) must have a person (referred to as the Records Custodian) with first-hand knowledge of the Electronic Signature process at the time the consumer is said to have signed the document. Each Records Custodian needs to have first-hand knowledge and be qualified to testify as to certain facts:

- how the Electronic Signature process worked at the time the offered document was signed or acknowledged,

- the basis for concluding that the record offered into evidence is a true and accurate copy of what was signed or acknowledged,

- the facts supporting the claim that the consumer (or the person against whom enforcement is sought) is the one who signed the record or acknowledged the disclosure,

- the information captured by the Audit Trail, and

- how the Tamper Seals on the Electronic Records works and show lack of tampering with the Electronic Records.

An Electronic Signature, e-delivery and Electronic Record archival process should be designed with these admissibility Legal Requirements in mind. If the admissibility Legal Requirements cannot be satisfied because there is not a person willing and qualified to testify to these matters, an insurer or Producer may be unable to enforce its position (in rescission actions, market conduct audits, or claim denials, for example).

Next, Best Practices will be reviewed, including how the Legal Requirements above may be satisfied.

BEST PRACTICES

Common to Insurers and Producers

Based on the Legal Requirements, below are a number of Best Practices for an insurer or Producer to consider in designing and implementing effective, compliant Electronic Signature, delivery and archival processes.

1. Start with a single business process and product line and create a process map for the ideal Electronic Signature, delivery and/or archival steps for that one business process and product.

2. If documents must be delivered electronically, determine how that will occur. For any e-delivery process, Electronic Records containing sensitive personal information should not be sent via email, whether in the email text or as an attachment. Instead, emails should be sent with links to a secure site, which invite the consumer(s) to access the secure website to retrieve such Electronic Records, which the Audit Trail captures. In addition:

a. Consider requesting the consumer's consent to accept all materials that may be provided via electronic delivery, to reduce the need to later ask for additional consent as the e-

delivery capabilities expand, (or for each specific electronic delivery, determine how consent will be achieved), and

b. Determine how to handle bounce-back or undelivered email. Consult the applicable insurance code on how to respond to notices of undelivered mail before determining whether to re-send via email or to initiate delivery via the USPS.

3. For the chosen process and product:

a. identify each form to be signed and/or delivered and categorize each form as:

i) a document to be provided that does not need to be signed and is not a Special Consumer Disclosure,

ii) a Special Consumer Disclosure not required to be signed by the consumer,

iii) a Special Consumer Disclosure that is required to be signed by the consumer, or

iv) a document that is not a Special Consumer Disclosure but is required to be signed,

and for each of the 4 categories, identify how the Legal Requirements summarized above will be met,

b. determine whether any forms in the process must be re-filed with any department of insurance (or for Producers, ask each appropriate insurer this question),

c. select an appropriate method to obtain the consumer's consent to sign electronically and Authenticate the identity of each person signing or receiving each Electronic Record, taking into account the motivation for a person to forge signatures in this area, as well as the harm caused by a forgery,

d. identify each document presented during the process and consider which other aspects of the process (such as IP address of the person signing, the time and date each step is completed) should be collected and recorded in the Audit Trail,

e. select the method for Tamper Sealing each Electronic Record immediately upon that record being signed by each person signing and for Tamper Sealing the Audit Trail, all which will support the Records Custodian's testimony on admissibility as well as on enforceability of the Electronic Records signed, as well as where and how each Electronic Record will be archived,

f. determine how to receive the consumers' perspective on the process, in particular to assure that the legal significance of each step is adequately and clearly explained in a way consumers will understand that they are signing legally significant documents, and

g. for those Special Consumer Disclosures identified in step 3(a) above, how will the ESIGN Consent be provided in accordance with the applicable insurance code Legal Requirements.

If the selected process will involve the use of voice signatures, consult with legal counsel familiar with ESIGN and UETA and the special considerations for voice signatures.

4. For each process:

a. before launching on a wide-scale basis, launch at least one pilot program to determine actual adoption of the process to solicit feedback on how to make the process more user friendly, without sacrificing quality, security, compliance, admissibility or enforceability, and

b. compare the risks of the proposed electronic process with the risks in the current traditional paper process, and adjust where appropriate.

5. Consider how the relevant records for a given policy owner or insured will be retrieved efficiently using a method where such records can withstand a Repudiation challenge, in response to actual or threatened litigation or regulatory examinations.

6. Before purchasing an electronic signature solution from a third party or developing the solution internally, be sure the proposed solution will be implemented in a way that meets all the Legal Requirements.

Specific for Insurers

1. Publish a set of requirements for those Producers who have or want to have their own Electronic Signature or electronic delivery process so they can perform due diligence in choosing and implementing a product and process that meets your company's requirements.

2. Develop an efficient method to review and verify Producers' requests for approval of their Electronic Signature or electronic delivery processes, such as requiring Producers to have an independent third party verify compliance.

3. Create a multi-disciplinary work group for the design of the processes, including representatives from IT, operations, new business, policyholder services, claims, legal, compliance, privacy and security areas, whether the process will be supported by an internally developed solution or one acquired from a vendor.

4. The work group should develop a common set of terms so all are clear on the meanings.

5. Seek active input from representative samples of Producers.

6. Consider the need to amend the company's current agreements or policies applicable to Producers, so that the Producers are properly informed of and bound to follow the company's e-contracting processes.

Specific for Producers

Request from insurers the requirements for an Electronic Signature or electronic delivery process and choose a vendor which meets those requirements as well as your preferred methods.

CONCLUSION

It has been over ten years since the legal framework for the use of Electronic Signatures and electronic delivery in the business of insurance was established nationally. Over those years, a number of practices have emerged to supplement the legal framework which should help the insurance industry embrace the opportunities available through the use of proven technology in this area.

A reasonably well designed electronic signature process, supported by the right technology, can actually reduce overall risk compared to paper processes. We hope that this paper will help ACORD members and the larger insurance community design the right processes to meet their particular needs to better serve the insurance buying public.

GLOSSARY

Audit Trail is a collective reference to the records containing the processes and details involved in each significant step of a given transaction, the process of each person accessing, completing, executing and transmitting each document to be acknowledged or signed in connection with the transaction, the process for authenticating each person for each document for that transaction and all documents executed or resulting from the process, all as sealed in a way that renders them tamper evident.

Authenticate or *Authentication* means the method used to verify that the person signing an Electronic Record is in fact the person he or she claims to be. This term is also used when discussing the rules of evidence and admissibility standards and in that context means the method of verifying that a given Record or document is in fact what it purports to be.

Best Practice means a legally compliant process, practice or method believed to be the preferred way of completing a given activity.

Digital Signature is a term that refers to a method of encrypting an Electronic Record using a hash value with a private key and may or may not be an Electronic Signature, which is form of signature in electronic form having legal significance.

Electronic Record means a contract or other record created, generated, communicated, received, or stored by electronic means.

Electronic Signature is, consistent with the definitions in ESIGN and UETA, an electronic symbol or process having legal significance and attached to, or logically associated with, a contract or other Record which is executed or adopted by a person with the intent to sign the Record, which does not necessarily need to be a process qualifying as a Digital Signature. A process where a person speaks his or her consent in a way that is associated with terms and conditions in a Record with an intent to be bound to those terms can be an Electronic Signature.

ESIGN means the Electronic Signatures In Global and National Commerce Act, 15 U.S.C §70001 et. seq., the federal Electronic Signature law.

ESIGN Consent means the disclosure required by ESIGN and several of the states' enactment of UETA to be provided to a "consumer," as defined by ESIGN or UETA as applicable, to which that consumer must consent as a condition to receiving one or more Special Consumer Disclosures exclusively via electronic means, where such consent is given in a way that reasonably demonstrates the consumer's ability to access information in the electronic form the Special Consumer Disclosures will be provided.

Legal Requirement means an act necessary to comply with applicable law, where the failure to take such act expose the person failing to take such act to adverse legal consequences, such as fines or other sanctions imposed by governmental authorities, the person being barred from enforcing his or her rights or defending himself or herself under the terms of a contract or disclosure that would have otherwise been enforceable had the person performed the acts in question.

Producer means the person or entity in a given transaction that is an agent, agency, broker, brokerage, insurance carrier, legally authorized individual or other entity that is sourcing consumers for insurance transactions for the respective insurer.

Repudiate means to challenge the enforceability of a given record or document on the basis that its terms were altered without the knowledge and consent of the person against whom enforcement of that record or document is sought.

Special Consumer Disclosure means information relating to a transaction or transactions which is required by a statute, regulation, or rule of law (other than ESIGN or UETA) to be provided or made available to a consumer in writing, which triggers the obligation to provide the special disclosure required to be provided under Section 101(c)(1) of ESIGN and the corresponding provisions in those seventeen states (as of the date of this paper) that have supplemented their enactment of UETA with the consumer consent provisions found in Section 101(c)(1) of ESIGN.

Tamper Seal, Tamper Seal Signatures and Tamper Evident Signatures mean a Digital Signature applied to an Electronic Record in a way that the record can be verified to ensure that no changes have been made to the Electronic Record since the seal was first applied.

UETA - the version of the Uniform Electronic Transactions Act, as published by the National Conference of Commissioners on Uniform State Laws and enacted in forty-seven states, as of the date of this paper (IL, NY and WA being the three that have not enacted UETA).

---

[1] Beyond the scope of this paper is the topic of when or if paper forms previously filed with the departments of insurance should be re-filed if electronic versions of those forms are created.

[2] ESIGN §101(c). As discussed below, 17 states of the 47 states that have enacted UETA (IL, NY and WA are the 3 states that have not enacted UETA) have also included in their enactment of UETA the special consumer disclosure provisions contained in the federal ESIGN. One state (PA) requires an affirmative consent to receive consumer disclosures solely through electronic means, which is just one step beyond what is required by UETA. Thus, twenty (20) states have the consumer protection provisions as stated in ESIGN Section 101(c).

[3] AK has expressly stated that its enactment of UETA shall not supersede the consumer disclosure provisions of ESIGN. Section 09.80.010(c).

[4] AL has recited the consumer disclosure provisions in the AL UETA. Section 8-1A-8(e).

[5] CO has incorporated by reference the consumer disclosure provisions of ESIGN. Section 24-71.3-103(6)(a).

[6] CT has expressly stated that its enactment of UETA shall not supersede the consumer disclosure provisions of ESIGN. Section 1-286.

[7] GA has expressly stated that its enactment of UETA shall not supersede the consumer disclosure provisions of ESIGN. Section 10-12-20.

[8] MD has expressly stated that its enactment of UETA shall not supersede the consumer disclosure provisions of ESIGN. Commercial Law, Section 21-102(f).

[9] MA has expressly stated that its enactment of UETA shall not supersede the consumer disclosure provisions of ESIGN. Chapter 110G, Section 3(b)(3).

[10] NH has expressly stated that its enactment of UETA shall not supersede the consumer disclosure provisions of ESIGN. Section 294-E:3.

[11] NV has added as official comment No. 2 to Section 4 of its enactment a comment that the consumer protection provisions in ESIGN shall apply. Section 919.210.

[12] NC has recited the consumer disclosure provisions in the NC UETA. Section 66-308-16(c).

[13] NJ has recited the consumer disclosure provisions in the NJ UETA. Section 12A:12-21.

[14] OR has recited the consumer disclosure provisions in the OR UETA. Section ORS Section 84.070.

[15] SC has expressly stated that its enactment of UETA shall not supersede the consumer disclosure provisions of ESIGN. Section 26-6-30(B)(2)(c).

[16] TN has expressly stated that its enactment of UETA shall not supersede the consumer disclosure provisions of ESIGN. Section 47-10-122.
[17] VT has recited the consumer disclosure provisions in the VT UETA. Section 287.
[18] WV has recited the consumer disclosure provisions in the WV UETA. W Va. Code Section 39A-2-1.
[19] WI has expressly stated that its enactment of UETA shall not supersede the consumer disclosure provisions of ESIGN. Section 137.12(2p).
[20] While the focus of this section of this paper is on Special Consumer Disclosures, the point in this paragraph applies to other records required to be provided, delivered or made accessible to consumers.