"New Strategic Analysis: *Guidelines for e-Signature and e-Delivery in the Insurance Business"* by Lock Lord, LLP; commissioned by ACORD

Summary by: Jeanette Griswold and Tom Scrivner

Summary

In order to better understand the legal requirements for Electronic Signatures and Electronic Delivery, ACORD commissioned Locke Lord, LLC to strategically analyze ESIGN (Electronic Signatures in Global and National Commerce Act) and UETA (Uniform Electronic Transactions Act). Below you will find a brief summary of the report. For more information please see the full report (attached). We hope that this report will allow more agencies to incorporate Electronic Signatures and Electronic Documents in order to provide more streamlined customer experiences.

Legal Requirements:

- ESIGN and UETA give legal legitimacy to Electronic Records and Electronic Documents to satisfy the "in writing" legal requirements for transactions. ESIGN and UETA permit companies to satisfy statutory record retention requirements solely through the use of Electronic Records.
- ESIGN and UETA require each person's consent to conduct business electronically. These laws also permit using Electronic Signatures and Electronic Records for consumer disclosers.
- Especially pertaining to the insurance industry: these laws do NOT apply to documents relating to wills, codicils or testimony trusts. This is relevant in estate planning techniques that involve life insurance and testamentary trusts. This also relates to health insurance and benefits of life insurance because notice of termination of benefits may not be given solely via e-delivery.

Difference Between ESIGN and UETA

- After ESIGN was enacted states were able to enact model versions of UETA. If a state has adopted their own version of UETA then their laws govern. However, if a state has not adopted a version of UETA then ESIGN laws will govern. Washington, Illinois, and New York are the only states that have not enacted UETA.

Electronic Signatures and Electronic Records Legal Status

- ESIGN and UETA state that signatures and records that are required to be "in writing" may not be denied solely because they are electronic.
- Electronic Signatures and Electronic Records have legal legitimacy but they do not have any special status.
- For example: when an insurance code requires an application for insurance to contain certain information, the electronic form of that application must contain that same information.

Security

- Privacy laws and data security laws apply to Electronic Records. Sensitive information such as health records and social security numbers must only be transmitted through secure channels.

Consumer Disclosures

- In insurance there are many circumstances when a Producer is required to inform a consumer of a certain aspect of their coverage and have the consumer initial or sign a document to that affect (ex: informing of availability of uninsured/underinsured motorist coverage). In these cases an Electronic Signature will satisfy those legal requirements.
- ESIGN and UETA allow all consumer disclosures to be provided via e-delivery. However, the consumer must be informed that they will be receiving documents electronically and the consumer must reasonably demonstrate their ability to open the e-disclosure in

the format that it will be delivered. The consumer must receive the e-disclosure form and sign it before the application for insurance can be signed.

    - One way to inform the client would be to provide a statement like this at the end of the email: *"I agree to complete this transaction electronically and to receive this and future disclosures and documents electronically. I have the capability to receive and open PDF documents on my computer."*
    - Once the client has emailed the signed document back they have demonstrated their ability to open the document.
- All e-documents must be made available to the consumer in a secure manner (ex: emailed to their personal email or available on a secure website).

Voice Signatures

- A voice signature can be used in regards to a consumer agreeing to use e-delivery, however, the recording must be attached to or logically associated with the record containing the terms with which the consumer is agreeing.

Record Retention Requirements

- When using Electronic Records for record retention purposes the records must be securely archived and properly indexed so that a person who is entitled by law can view them in a timely manner.

Authentication and Fraud Prevention

- Companies should use authentication procedures in order to prevent forged Electronic Signatures. Companies can do this by asking a secret question or requiring the consumer to enter personal information (driver's license number, Social Security number, etc).
- Companies should match the Authentication steps according to the risk of forgery to the type of transaction.
- Neither ESIGN nor UETA specify methods of Authentication but Locke Lord, LLC consider it as a legal requirement rather than just best practices.
- In order to protect your company and the consumer from tampered documents it is recommended that you utilize an Audit Trail or Tamper Seal software. This software

allows you to view the history of the document including any changes that were made to it.

- Neither ESIGN nor UETA specify methods of Authentication but Locke Lord, LLC consider it as a legal requirement rather than just best practices.

"Docusign" has been catering heavily to independent agents as a software company that can provide authentication and fraud protection services. "EchoSign" has been used by IIA of Texas in the past for authentication and fraud protection.
IIABAZ does not endorse or recommend either of these companies.

Admissibility Requirements

- A company seeking to enforce terms and conditions in a record must have a person (Records Custodian) that has first-hand knowledge of the Electronic Records and Electronic Signature process from the time that the documents were signed. The Records Custodian must be able to testify to these facts:
    - How the Electronic Signature process worked at the time of the questioned record
    - How he/she may conclude that the record is a true and accurate copy
    - The ability to show that the consumer was the person that signed/acknowledged the record
    - Present and explain the information in the Audit Trail
    - Present and explain the Tamper Seal and show that the record has not been tampered with

For step-by-step instructions on how to get started using Electronic Signatures and Electronic Records please see the full report on our website www.iiabaz.com .