

ELECTRONIC TRANSACTIONS: The Law Today and Court Decisions on Electronic Transactions



Wanda Borges, Esq.
Borges & Associates, LLC

I. INTRODUCTION

Electronic transactions have become an essential component of commercial activity, legal practice, and everyday life. As attorneys, understanding the statutory frameworks that govern electronic signatures and records – and the rapidly developing judicial interpretations surrounding them – is now indispensable. This article provides an overview of the governing law, recent case trends, and the evidentiary burdens attorneys must anticipate when enforcing or challenging electronic transactions.

II. STATUTORY FRAMEWORK

A. Foundational Principles

The Uniform Electronic Transactions Act and the Electronic Signatures in Global and National Commerce Act [15 USC 7001 et seq] form the backbone of U.S. electronic transaction law.

B. Electronic Signatures in Global and National Commerce Act (“E-Sign”)

15 USC 7001 *et seq* The Electronic Signatures in Global and National Commerce Act (“E-Sign”), in pertinent part provides:

(a) In general

Notwithstanding any statute, regulation, or other rule of law (other than this subchapter and subchapter II), with respect to any transaction in or affecting interstate or foreign commerce—

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

(b) Preservation of rights and obligations

This subchapter does not—

(1) *limit, alter, or otherwise affect any requirement imposed by a statute, regulation, or rule of law relating to the rights and obligations of persons under such statute, regulation, or rule of law other than a requirement that contracts or other records be written, signed, or in nonelectronic form; or*

(2) *require any person to agree to use or accept electronic records or electronic signatures, other than a governmental agency with respect to a record other than a contract to which it is a party.*²

The E-Sign Act provides for substantial disclosures and protections in connection with consumer transactions. 15 USC 7001(c) is excerpted herein:

(c) Consumer disclosures

(1) Consent to electronic records. *Notwithstanding subsection (a), 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 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 E-Sign Act provides additional rights for a consumer which one can find in 15 USC 7001 (c)(2), the most pertinent of which is:

(B) Verification or acknowledgment. *If a law that was enacted prior to this chapter 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).*³

One area of the E-Sign Act which became more used and effective following the pandemic is 15 USC 7001(g) which states:

(g) 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.*⁴

² 15 U.S.C. §7001(b)

³ 15 U.S.C. §7001(c)

⁴ 15 U.S.C. §7001(g)

Section 7002 of the E-Sign Act provides that any state may displace the E-Sign Act if the Uniform Electronic Transactions Act (“UETA”) is adopted.

Section 7003 of the E-Sign Act specifically excludes certain contracts or documents relating to

- Wills, codicils, and testamentary trusts
- Family law matters (divorce, adoption)
- Court orders and notices
- Certain foreclosure and eviction notices
- Notices of utility termination, health insurance cancellation, or product recalls
- the Uniform Commercial Code, as in effect in any State, other than sections 1-107 and 1-206 and Articles 2 and 2A.⁵

C. The Uniform Electronic Transactions Act (“UETA”)

UETA has been adopted by 49 states (all except New York), as well as D.C., Guam, Puerto Rico, and the U.S. Virgin Islands. New York instead uses the Electronic Signatures and Records Act (“ESRA”).

Most states have codified UETA within their Business and Commerce Codes. The portions of UETA set forth below are taken directly from the Final version of the Uniform Electronic Transactions Act (1999) as found on the Uniform Law Commission website. (www.uniformlaws.org)

This Act was originally approved by the American Bar Association on February 14, 2000. Generally, the language of UETA, adopted by the 49 states is identical to this version.

Similar to the E-Sign Act, UETA excludes contracts or documents relating to wills, codicils, and testamentary trusts, the UCC other than Article 2 and 2A, and other laws which each state may identify. UETA applies to commercial and consumer transactions and “ensures that contracts and records created electronically hold the same legal weight as their paper counterparts, streamlining business operations and personal agreements.”⁶

It is important to note that while a contract and record can be created electronically, there must be evidence to prove that each of the parties agreed to conduct an electronic transaction; and consent to conduct one transaction electronically is not a blanket agreement to conduct all transactions electronically. UETA provides in pertinent part:

Use of Electronic Records and Electronic Signatures (Section 5)

(a) This Act does not require a record or signature to be created, generated, sent, communicated, received, stored, or otherwise processed or used by electronic means or in electronic form.

(b) This Act applies only to transactions between parties, each of which has agreed to conduct transactions by electronic means. Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties’ conduct.

(c) A party that agrees to conduct a transaction by electronic means may refuse to conduct other transactions by electronic means. The right granted by this subsection may not be waived by agreement.

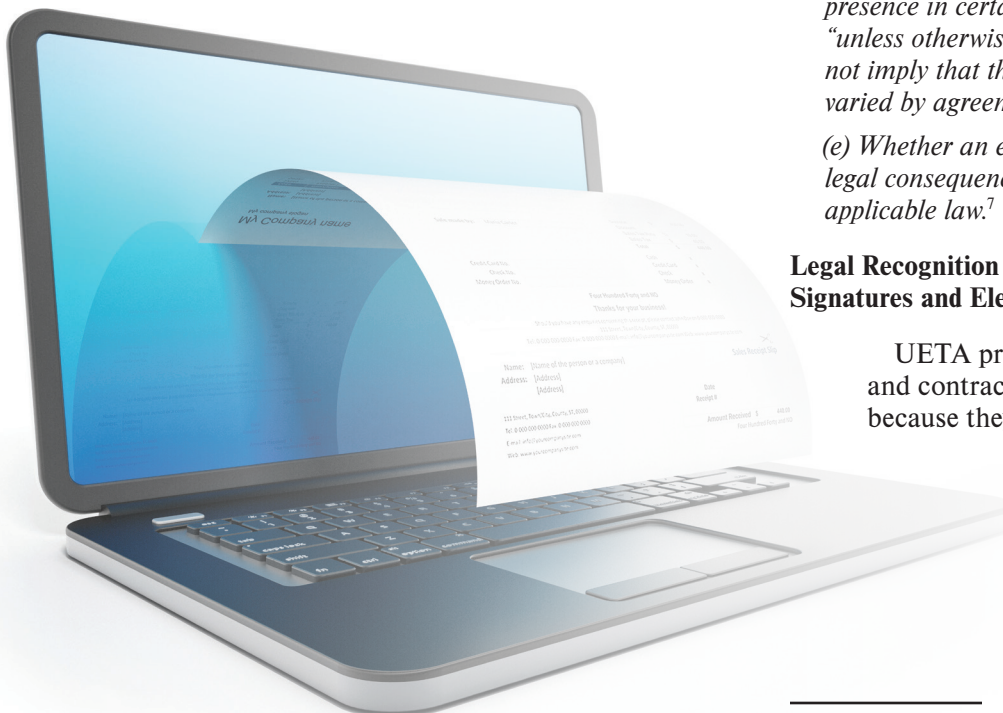
(d) Except as otherwise provided in this Act, the effect of any of its provisions may be varied by agreement. The presence in certain provisions of this chapter of the words “unless otherwise agreed,” or words of similar import, does not imply that the effect of other provisions may not be varied by agreement.

(e) Whether an electronic record or electronic signature has legal consequences is determined by this Act and other applicable law.⁷

Legal Recognition of Electronic Records, Electronic Signatures and Electronic Contracts. (Section 7)

UETA provides that electronic records, signatures and contracts will not be denied enforceability because they are in an electronic format and states:

(a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.



⁵ See 15 U.S.C. §7003

⁶ Legalclarity.org March 21, 2025, issue article titled “Texas Uniform Electronic Transactions Act: Key Legal Considerations”

⁷ UETA Section 5

(b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

(c) If a law requires a record to be in writing, an electronic record satisfies the law.

(d) If a law requires a signature, an electronic signature satisfies the law.⁸

Generally, the six factors which the court will consider in determining whether or not an electronic transaction is enforceable are: Attribution, Authentication, Consent, Intent, Security, and Record Retention. Most of these are specifically addressed by UETA. Caselaw relies on these factors, as will be discussed below.

Attribution (Section 9)

UETA provides:

Attribution and Effect of Electronic Record and Electronic Signature

(a) An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.

(b) The effect of an electronic record or electronic signature attributed to a person under Subsection (a) is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement, if any, and otherwise as provided by law.⁹

Retention of Electronic Records (Section 12)

(a) If a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record which:

(1) accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise; and

(2) remains accessible for later reference.

(b) A requirement to retain a record in accordance with Subsection (a) does not apply to any information the sole purpose of which is to enable the record to be sent, communicated, or received.

(c) A person may satisfy Subsection (a) by using the services of another person if the requirements of that subsection are satisfied.

(d) If a law requires a record to be presented or retained in its original form or provides consequences if the record is not presented or retained in its original form, that law is satisfied by an electronic record retained in accordance with Subsection (a).

(e) If a law requires retention of a check, that requirement is satisfied by retention of an electronic record of the information on the front and back of the check in accordance with Subsection (a).

(f) A record retained as an electronic record in accordance with Subsection (a) satisfies a law requiring a person to retain a record for evidentiary, audit, or like purposes, unless a law enacted after January 1, 2002, specifically prohibits the use of an electronic record for the specified purpose.

(g) This section does not preclude a governmental agency of this state from specifying additional requirements for the retention of a record subject to the agency's jurisdiction.¹⁰

III. WHAT THE COURTS EMPHASIZE

A. Intent to Sign and Adopt a Record

Courts evaluate whether an electronic signature represents an individual's **intent to authenticate** a document. Under revisions to the UCC, "authentication" includes adopting a symbol, encrypting, or otherwise processing a record with intent to identify oneself.

Thus, platforms that clearly capture the user's affirmative action – clicking "I agree," applying a typed signature, or using secure credentialed login – tend to withstand scrutiny.

UETA clearly requires intent. "Electronic signature" is defined as an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. (emphasis added)

B. Agreement to Conduct Business Electronically

Judges frequently examine **whether the parties intended to transact electronically**, a requirement found in UETA. In conducting this examination courts will need to determine 1) whether the electronic process was obvious and transparent, 2) whether terms and conditions were accessible, and 3) whether the user had a reasonable opportunity to review them.

C. Reliability of the Electronic System

Courts consider whether the system producing the electronic signature is reliable and secure. Evidence such as audit trails, timestamps, IP logs, and platform procedures becomes central in litigation involving the authenticity of electronic signatures.

⁸ UETA Section 7

⁹ UETA Section 9

¹⁰ UETA Section 12

IV. BURDEN OF PROOF IN ENFORCING ELECTRONIC TRANSACTIONS

Enforcement often hinges not on the legality of electronic signatures, which is well established, but on **evidentiary sufficiency**. Recent decisions emphasize:

A. Proving the Electronic Signature's Authenticity

When the existence or validity of an electronic signature is challenged, the burden is on the proponent to show:

1. **The signature was made by the purported signer**, and
2. **The signer intended to authenticate** the record.

This can be proven with system records, platform logs, user credential evidence, or demonstrating standard operating procedures of the electronic signature platform.

B. Demonstrating Parties' Consent to Electronic Contracting

Because UETA requires that parties intend to transact electronically, attorneys must show clear and consistent practices or explicit agreements. Evidence may include:

- Signed credit applications.
- Terms incorporated by reference (such as website terms)
- Confirmations, invoices, purchase orders, and communications forming a full contract package.

C. Evidentiary Challenges in Litigation

Courts expect a reliable record keeping system. Missing metadata, inconsistent timestamps, or unverifiable audit data can jeopardize enforceability. Conversely, robust electronic documentation strongly supports motions for summary judgment.

V: CASELAW

Aerotech, Inc. v. Boyd, 624 S.W.3d 199 (Tex. 2021)

Supreme Court of Texas is the leading case from Texas on the Attribution requirement for electronic signatures under Tex. Bus. & Com. Code §322.009. *Aerotech* is widely recognized throughout the country as a leading case on the Attribution requirement.

Facts: Aerotech, a staffing company, used an online only hiring application for onboarding employees. Applicants received an email link, created unique login credentials, and completed the process by electronically signing required documents, including an Electronic Disclosure Agreement (EDA) and a Mutual Arbitration Agreement (MAA). The system recorded timestamps and other audit data and did not allow completion of the application unless all required documents were electronically signed. Four employees completed the onboarding process, were later terminated, and sued Aerotech for racial discrimination and retaliation. Aerotech moved to compel arbitration based on

the electronically executed MAAs. The employees acknowledged completing the online application but denied ever seeing or signing the arbitration agreements. The trial court denied Aerotech's motion to compel arbitration. A divided panel of the court of appeals affirmed rejecting Aerotech's argument that it had conclusively established the MAAs' validity. Interestingly, the dissent "took issue with the majority's analysis, arguing that it set 'a standard that would make electronic contract formation practically impossible and write section 322.009 out of the law.'"¹¹

The Supreme Court granted Aerotech's petition to review. The employees conceded that they completed Aerotech's computerized hiring application and electronically signed the documents except for the MAAs but had provided no evidence to support the allegation that they did not electronically sign the MAAs. The employees claimed that Aerotech had not established the efficacy of the hiring application's security procedures. Aerotech, on the other hand, had adduced testimony from its program manager, Phaedra Marsh, who helped design and develop the application. Marsh's had testified that the employees would have to complete everything before the final application could be signed and completed. Additional testimony was given by an administrative assistant who was at Aerotech to help employment candidates to finish the application through the "finalize and submit process". The employees offered nothing other than a bare denial that the MAAs had not been signed.

Holding: The Texas Supreme Court held that Aerotech conclusively established that the employees electronically signed the arbitration agreements, and that a bare denial of signing is insufficient as a matter of law to defeat attribution once the efficacy of the electronic security procedures is shown. Under Tex. Bus. & Com. Code § 322.009, an electronic signature is attributable to a person if it is shown to be that person's act, including by demonstrating the efficacy of security procedures.

- Aerotech presented detailed evidence explaining how its system worked, including unique user IDs and passwords, required sequential execution of documents, audit trails, and timestamps.
- The Court emphasized that the employees offered no affirmative evidence of unauthorized access, system malfunction, or credential compromise—only denials.
- The Court concluded that mere denial does not create a fact issue once attribution is established through reliable security procedures.

Houston ANUSA, LLC v. Shattenkirk, 693 S.W.3d 513 (Tex. App. 2023)

Facts: This case is similar to the *Aerotech*. A terminated employee sued AutoNation, the employer, for discrimination and retaliation. The employer filed a motion to compel arbitration based on an electronically signed

¹¹ *Aerotech v. Boyd*, 624 S.W. 3d 199 (2021) citing 2019 WL 4025040 (Tex. App. - Dallas 27, 2019)



arbitration agreement that was part of the onboarding process. The employee stated that the arbitration agreement was not valid because he had not signed it through electronic means. The trial court relied heavily on the *Aerotek* decision. First and foremost, it determined that AutoNation “as proponent of the arbitration agreement bears both the initial burden of establishing the agreement’s existence by legally sufficient evidence and of negating any contravening evidence from” the employee.¹² The Court of Appeals examined whether AutoNation “had provided sufficient evidence to establish that the electronic transaction security procedures were sufficient to establish the genuine nature of Shattenkirk’s signature on the electronic contract in accordance with” the Texas UETA.¹³ The Court reviewed the affidavit of AutoNation’s Human Resources manager which set forth the process that purportedly led to the employee’s electronic signing of the arbitration agreement. The Court also reviewed the affidavit of the employee in support of his position that he never agreed to be bound by the arbitration agreement.

Holding: The Texas Court of Appeals held that the affidavit of AutoNation’s Human Resources manager did not conclusively establish the security procedures used by AutoNation in their onboarding process. Also, AutoNation failed to conclusively establish the efficacy of the security procedures, it did “furnish more than a scintilla of evidence showing Shattenkirk’s consent to the agreement.”¹⁴ Turning then to Shattenkirk’s evidence. His declaration completely denied completing any employment document electronically. He averred that he completed the employment documents manually. The Court concluded that his “denial of completing any agreements electronically is some evidence that he did not consent to the arbitration agreement through use of an electronic signature.”¹⁵ The Court concluded that there was a fact issue regarding whether Shattenkirk had consented to the arbitration agreement by electronic signature and that would have to be decided by an evidentiary. Thus, the matter was remanded to the trial court.

¹² *Houston ANUSA, LLC v Shattenkirk*, 693 S.W. 3d 513 (2023), citing *Rachal*, 403 S.W. 3d at 843; *In Estate of Guerrero*, 465 S.W. 3d 693, 699 (Tex. App. – Houston [14th Dist.] 2015, pet denied)

¹³ *Houston ANUSA, LLC v Shattenkirk*, 683 S.W. 3d 513 (2023)

¹⁴ *id*

¹⁵ *id*

Designs for Health, Inc. v Miller, 187 Conn. App 1 (Appellate Court of Connecticut) (2019)

Designs for Health, a producer of professional lines of nutraceutical and natural health products sued Miller, a podiatrist alleging that Miller had agreed to sell Designs for Health products and Miller violated that agreement. Neither Designs for Health nor Miller were physically located in Connecticut. Nevertheless, the contract contained a forum-selection clause. Miller moved to dismiss claiming the court lacked personal jurisdiction and that the plaintiff could not meet its burden to prove that he had signed the agreement. It was not disputed that the agreement was executed electronically “through a secure portal provided by a third-party known as ‘Docu-Sign’...” Miller denied those allegations but offered no independent evidence to refute them. The Defendant further contended that plaintiff’s documents were forgeries.

Holdings: The Superior Court in Connecticut granted the motion to dismiss based on Miller’s “direct, highly specific testimonial evidence” which supported his denials. On appeal, the Appellate Court relied heavily on the 2nd Circuit Court of Appeals decision in *Dorchester Financial Securities Inc. v. Banco BRJ, S.A.*, 722 f. 3d 81, finding that Connecticut practice was consistent with the Second Circuit jurisprudence. The Court concluded that the *prima facie* standard made sense in this case where the evidentiary record was only partially developed and the parties did not request a full evidentiary hearing. The Court upheld the contract containing a forum selection clause finding that DocuSign’s certificate of completion was *prima facie* evidence that the defendant signed the document on the date and time stated. The Plaintiff was found to have met its burden of proof. If the Defendant had requested an evidentiary hearing on the evidence, the result might have been different.

Conduent Commercial Solutions, LLC v. Boren 2025 WL 1208685 (Tex. App. April 2025)

Facts: In this case, the employee Boren, suffered an injury on her job shortly after commencing work at Conduent Commercial Solutions. She sued for damages resulting from her injury and Conduent field a motion to compel arbitration, arguing that Boren signed an

Acknowledgment that contained an arbitration provision. The Court cited to the Tex. Bus. & Com Code §322.009(a) and said that “An electronic signature is attributable to a person if it was the act of the person and the act of the person ‘may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.’” The Court also referred to Section 322.002(13) which defines a security procedure as any “procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record”¹⁶. The Court noted the instructions from the *Aeroteck* decision that said “[S]ecurity procedures may include requiring personal identifying information—such as a social security number or an address—to register for an account; assigning a unique identifier to a user and then tying that identifier to the user’s actions; maintaining a single, secure system for tracking user activities that prevents unauthorized access to electronic records; business rules that require users to complete all steps in a program before moving on or completing it; and timestamps showing when users completed certain actions. These examples are illustrative and not exclusive under Section 322.009(a).”¹⁷ Conduent asserted that it presented sufficient evidence to satisfy the non-exclusive examples in section 322.009(a). Both sides agreed that the *Aeroteck* decision is controlling.

Holding: The affidavit presented by Conduent was made by the Senior Director of Global People Relations with no statement as to her responsibilities, experience or any knowledge of Conduent’s onboarding or security procedures. The Court found that Conduent “failed to produce (1) evidence from anyone with personal knowledge of its security procedures at the time it hired Boren, (2) evidence showing Boren signed the Acknowledgement, (3) evidence of its capacity to detect changes or errors in its electronic records, (4) evidence of the application’s business rules, and (5) the reliability or up-time of relevant programs; instead, it produced evidence conclusively demonstrating its offer letter was modified and revealing unexplained differences between its offer letter and the Acknowledgement.”¹⁸ Conduent’s motion to compel arbitration and request for a stay was denied.

Lorraine v. Markel American Ins. Co. 241 F.R.D 534 (U.S.D.C. MD 2007)

This case was brought to enforce an arbitrator’s award and both parties sought summary judgment. The basis for the litigation was to determine the scope of the arbitration agreement. This case centered on the admissibility of electronically stored information (**ESI**) under the Federal Rules of Evidence (**FRE**). *Lorraine* is widely regarded as the most comprehensive judicial analysis of ESI

admissibility. The opinion was clear that whenever ESI is offered as evidence, either at trial or in summary judgment, the following evidence rules must be considered: “(1) is the **ESI relevant** as determined by Rule 401 (does it have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be); (2) if relevant under 401, is it **authentic** as required by Rule 901(a) (can the proponent show that the ESI is what it purports to be); (3) if the ESI is offered for its substantive truth, is it **hearsay** as defined by Rule 801, and if so, is it covered by an applicable exception (Rules 803, 804 and 807); (4) is the form of the ESI that is being offered as evidence an **original** or **duplicate** under the original writing rule, of if not, is there admissible secondary evidence to prove the content of the ESI (Rules 1001-1008); and (5) is the probative value of the ESI substantially outweighed by the danger of **unfair prejudice** or one of the other factors identified by Rule 403, such that it should be excluded despite its relevance.”

Neither party was able to authenticate the ESI. There was no testimony from someone who created, maintained or used the system or record. There was no evidence as to how the computer system involved reliably created, stored or retrieved records. Hearsay could not be overcome. There was no showing that the ESI was either an original or permissible duplicate.

Holding: The Concluding paragraph of this court’s 50-page decision is the best summary. “In this case the failure of counsel collectively to establish the authenticity of their exhibits, resolve potential hearsay issues, comply with the original writing rule, and demonstrate the absence of In this case the failure of counsel collectively to establish the authenticity of their exhibits, resolve potential hearsay issues, comply with the original writing rule, and demonstrate the absence of unfair prejudice rendered their exhibits inadmissible, resulting in the dismissal, without prejudice, of their cross motions for summary judgment. The discussion above highlights the fact that there are five distinct but interrelated evidentiary issues that govern whether electronic evidence will be admitted into evidence at trial or accepted as an exhibit in summary judgment practice. Although each of these rules may not apply to every exhibit offered, as was the case here, each still must be considered in evaluating how to secure the admissibility of electronic evidence to support claims and defenses. Because it can be expected that electronic evidence will constitute much, if not most, of the evidence used in future motions practice or at trial, counsel should know how to get it right on the first try.”

Khoury v. Tomlinson, 518 S.W. 3d 568 (2017) (Texas Court of Appeals)

This case has become more important as emails are commonly used to create contracts and is frequently cited by other jurisdictions for this proposition. The email constituted a writing sufficient to enforce the making of a contract and overcome a claim that the Statute of Frauds prevented the contract from being enforced. There were

¹⁶ Tex. Bus. & Com. Code §322.022(13)

¹⁷ *Conduent Commercial Solutions, LLC v. Boren* 2025 WL 120685, citing to *Aeroteck v. Boyd*, 624 S.W. 3d 199 (2021)

¹⁸ *Conduent Commercial Solutions, LLC v. Boren* 2025 WL 120685

several issues in this appeal. This article will address only the question of an electronic record.

Facts: Khoury was an investor in PetroGulf, of which Tomlinson was the president. There is no dispute that an investment document was created by which Khoury invested \$400,000 in PetroGulf. The investment funds were obtained by Khoury taking out a loan from Garantia Financiera Vital y Accidentes S.A. Khoury became dissatisfied with the investment and wanted the return of his money. A meeting was held on January 9, 2012, during which Tomlinson agreed to repay the debt over a four- or five-year period. A week later, Khoury sent an email to Tomlinson detailing the terms of the agreement and requesting confirmation by Tomlinson of the agreements. Tomlinson replied, in writing, “We are in agreement.” No payments were made. Although Tomlinson admitted at trial that the email had been sent, his claim was that the email referred to a completely different agreement. He also argued that the email was not signed and therefore, the Statute of Frauds applied and there could be no binding contract unless it was in “writing”. The trial court found in favor of Khoury that Tomlinson had breached the agreement and was required to repay the \$400,000.00.

Holding: The court found that the email correspondence is governed by the Texas Uniform

Electronic Transactions Act (“UETA”). Citing the Tex. Bus. & Com. Code §322.001 – 021, it noted that UETA “applies to electronic records and signatures relating to a transaction” and that a record or signature may not be denied legal effect or enforceability solely because it is in electronic form.” The court said “We must construe and apply UETA in a manner “to be consistent with reasonable practices concerning electronic transactions and with the continued expansion of those practices.”¹⁹ The Court found that the evidence established that the parties intended to be bound by the terms of the agreement and that an agreement had been made by the email saying “We are in agreement.” It was found that this language “clearly and unambiguously expresses the intent to be bound by terms of their agreement...that Tomlinson signed the email and that the signed email satisfies the Statute of Frauds.”²⁰

Zulkiewski v American General Life Ins. Co. 2012 WL 2126068 (Michigan Court of Appeals)

This appeal was brought by disgruntled former beneficiaries of Zulkiewski. *American General* received an electronic beneficiary change through its online system. Upon the death of Zulkiewski, both the beneficiaries and the former beneficiaries claimed the proceeds of the life insurance policy.

Facts: An online account was established providing all the required information and was thereafter used to change the beneficiaries. To enroll in the service, the applicant apparently was required to enter decedent’s policy number, social security number, mother’s maiden name, and an

e-mail address. The applicant then chose a password and verified it. An email was then sent to the policy-holder advising that he had enrolled in eService and warned him to contact the insurance company immediately if he did not intend to enroll in that service. Upon the death of the policyholder, American General remitted the life insurance proceeds to the substituted beneficiary. The former beneficiaries argued that the insurance company could not prove the efficacy of its security procedures.

Key Legal Issues: 1) Was the transaction enforceable under UETA?; 2) Did the electronic beneficiary change satisfy the policy’s requirement of “written notice”?; 3) Did American General establish that the requirements of UETA had been followed?

Holding: In support of the electronic signature plaintiff and American General submitted evidence concerning the safeguards used to sign up for the eService system and those used during the subsequent beneficiary change. As noted by the trial court, these safeguards consisted of not only knowledge of various items of decedent’s personal information, including having access to the insurance policy number, his social security number, his mother’s maiden name, and an email address, but also of e-mail and regular mail notifications after the initial establishment of the e-Service account and the subsequent beneficiary change. An affidavit was submitted showing that the substitute beneficiary lacked any involvement in making the disputed change. The court also accepted that affidavit to find that the decedent was highly computer-literate and had also made plaintiff the beneficiary of other insurance policies. The Court of Appeals found that American General had met their burden under the Michigan UETA and that appellants offered nothing more than conjecture. The trial court did not err in awarding the insurance proceeds to the substitute beneficiary.

VI. CONCLUSION

The legal landscape surrounding electronic transactions is both stable – thanks to UETA and E SIGN – and evolving due to the steady stream of judicial interpretation. Courts continue to accept electronic signatures as valid and enforceable, but they rigorously evaluate the evidence establishing authenticity, system reliability, and the parties’ intent. Attorneys who understand these contours and prepare evidentiary foundations accordingly will be well positioned to enforce electronic agreements effectively. ■

¹⁹ *Khoury v. Tomlinson*, 518 S.W.3d 568 (2017), citing Tex. Bus. & Com. Code §322.006(2)

²⁰ *Khoury v. Tomlinson*, 518 S.W. 3d 568 (2017)