Strafford

Presenting a live 90-minute webinar with interactive Q&A

E-Signatures and Electronic Loan Documentation in Real Estate Finance: ESIGN and UETA, Interplay With UCC

Enforceability, Authentication, and Admissibility; MERS and Transferability

THURSDAY, FEBRUARY 13, 2020

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Ankush R. Israni, Attorney, **Stroock & Stroock & Lavan LLP**, Los Angeles

Andrei D. Tsygankov, Partner, **Bekiares Eliezer LLP**, Atlanta

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-877-447-0294** and enter your **Conference ID and PIN** when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the 'Full Screen' symbol located on the bottom right of the slides. To exit full screen, press the Esc button.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 2.

Program Materials

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the link to the PDF of the slides for today's program, which is located to the right of the slides, just above the Q&A box.
- The PDF will open a separate tab/window. Print the slides by clicking on the printer icon.

The Legal Challenges in e-Signatures: Key Pointers to Ensure Validity

Ankush R. Israni
Attorney
Stroock & Stroock & Lavan LLP
aisrani@stroock.com

Andrei D. Tsygankov
Partner
Bekiares Eliezer LLP
atsygankov@founderslegal.com

What We Will Cover Today

I. Introduction to ESIGN and UETA

II. Electronic signatures: What are they?

III. ESIGN and UETA in practice

IV. Remote Notarization & eNotarization

V. MERS: mortgage industry infrastructure established to support eNotes

VI. Creating and transferring ownership of eNotes

VII. Post-closing: the role of the document custodian for electronic files

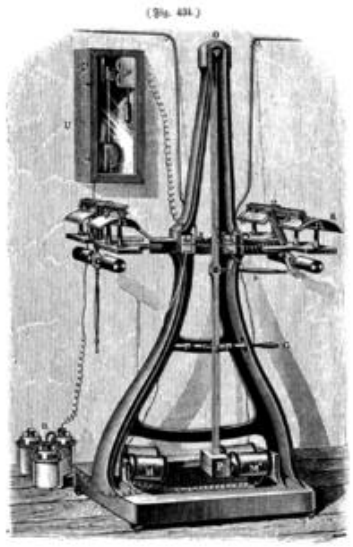
VIII. State law concerns: UCC and recordable instruments

IX. Admissibility of electronic signatures and documents into evidence

I. Introduction to ESIGN and UETA

Earliest Instances of 'E-Signatures'

- The first widely-used system for sending signatures across large distances was finalized in 1862, through a device named the "Pantelegraph".
- Pantelegraphs sent signatures or small drawings over existing telegraph lines.
- The very first transmission carried a signature over 80 miles in less than two minutes.



Relevant E-Signature Laws

Electronic Signatures in Global and National Commerce Act (ESIGN)

- 15 U.S.C. §§ 7001-7031
- Passed into Federal Law in 2000

Uniform Electronic Transactions Act (UETA)

- Model law drafted by the National Conference of Commissioners on Uniform State Laws to prevent non-uniformity
- Presented for adoption by individual states in 1999

Electronic Signatures in Global and National Commerce Act (ESIGN) – An Overview

ESIGN is the Federal solution:

- Applies to all US States and Territories
- Creates a national baseline for the use of electronic signatures and records
- Provides specific requirements for consumer transactions
- Sets boundaries for regulatory authority
- Is technology-agnostic
- Preempts inconsistent state laws

ESIGN – General Principles

1. A record or signature may *not* be denied legal effect or enforceability *solely* because it is in electronic form.
2. A contract relating to a transaction may *not* be denied legal effect or enforceability *solely* because an electronic record was used in its formation.
3. If a law requires a record to be in writing, an electronic record satisfies the law.
4. If a law requires a signature, an electronic signature satisfies the law.
5. In a proceeding, evidence of a record or signature may *not* be excluded *solely* because it is in electronic form.

ESIGN – General Principles

ESIGN applies only to Transactions:

- That affect Interstate Commerce
- That involve Foreign Commerce
- With the Federal Government

What is a "**Transaction**"?

- Sale, lease, exchange, licensing or other disposition of personal property, goods, intangibles, services or combination thereof;
- Sale, lease, exchange or other disposition of any interest in real property.

ESIGN – General Principles

ESIGN does **NOT** require any person to use or accept electronic records or signatures.

- If parties agree to electronic signatures, then ESIGN gives them legal effect.
- In Business-to-Business (B2B) transactions, prior behavior among the parties can govern acceptance of electronic signatures and records.
- In Business-to-Consumer (B2C) transactions, Consumers must have notice, and must consent to electronic signatures.

ESIGN – General Principles

If the law requires that a contract or other record must be in writing to have legal effect, validity or enforceability, electronic form **MAY** be denied if:

- Such record cannot be retained and accurately reproduced by all parties.

ESIGN – Exclusions

1. Substantive protections provided by consumer protection laws.
2. Content or timing of disclosures required by law.
3. Any requirement by a federal regulatory agency, self-regulatory organization, or state regulatory agency that records be filed in a specified standard.

NOTE, HOWEVER: 21st Century Integrated Digital Experience Act (IDEA) of 2018

ESIGN – Exclusions

4. Any contract governed by:
   - (a) A statute, regulation, or other rule of law governing the creation and execution of **wills**, **codicils, or testamentary trusts**.
   - (b) A State statute, regulation, or other rule of law governing adoption, divorce, or other matters of **family law**.
   - (c) the Uniform Commercial Code **(UCC)**, as in effect in any State, *other than* sections 1–107 and 1–206 and Articles 2 and 2A.

ESIGN – Exclusions

5. Court orders or notices, or official court documents (including briefs, pleadings, and other writings) required to be executed in connection with court proceedings.

6. Any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.

ESIGN – Exclusions

7. Any notice of:

   - (a) the cancellation or termination of utility services (including water, heat, and power).
   - (b) 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.
   - (c) the cancellation or termination of health insurance or benefits or life insurance benefits (excluding annuities).
   - (d) recall of a product, or material failure of a product, that risks endangering health or safety.

Uniform Electronic Transactions Act (UETA) – An Overview

UETA is the State solution:

- Model law presented to states to codify into state law.
- Establishes that electronic signatures have the same legal authority as 'wet' signatures.
- Adopted by 47 states, D.C., Puerto Rico, U.S. Virgin Islands. *Exceptions*:
  - Illinois
  - New York
  - Washington

UETA – General Principles

1. ESIGN has provided the States with an option to enact UETA *substantially as written*, or face pre-emption by ESIGN Act
2. If state adopted UETA in substantially Model form, the state's law would prevail over ESIGN
3. If a state's UETA provision is inconsistent with ESIGN, the Federal law would again pre-empt as to that provision.

UETA – General Principles

UETA:

- Does not change contract law.
- Supplements contract law, to permit parties to transact business electronically.
- As supplemented by UETA, the law of contract formation, the basic elements of validity and verification of inked signatures continue in the electronic signature realm, albeit with some additional considerations.

II. Electronic Signatures: What Are They?

Electronic Signatures: What Are They?

What is "**electronic**"?

- Relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

What is an "**electronic signature**"?

- The signature may be a sound, symbol, or process.
- The signature must be attached to or logically associated with an electronic record that was signed.
- The signature must be made with the intent to sign the electronic record.

Electronic Signatures: What Are They?

What is a "**record**"?

- Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

What is an "**electronic record**"?

- A record created, generated, sent, communicated, received, or stored by electronic means.

Comment 6 to UETA Section 2

- "Information processing systems, computer equipment and programs, electronic data interchange, electronic mail, voice mail, facsimile, telex, telecopying, *scanning*, and similar technologies all qualify as electronic under this Act."

Electronic Signatures: What Are They?

- **E-Signature Examples:**

  - Providing a scanned image of a handwritten signature that is attached to an electronic document.
  - Using a computer mouse to click on an “I agree” button.
  - Signing a store receipt on an electronic pad.
  - Providing a secret code, password, or PIN to identify the sender to the recipient.
  - Providing a unique biometrics-based identifier, such as a fingerprint, voice print, or a retinal scan.
  - Creating a sound, such as the sound by pressing “9” on a telephone, to indicate acceptance.
  - Typing the sender’s name at the end of an email message.

III. ESIGN and UETA In Practice

ESIGN & UETA In Practice

Written agreement in downloadable, electronic form is valid.

"…agreement is a "written provision" despite being provided to users in a downloadable electronic form. The latter point has been settled by the Electronic Signatures in Global and National Commerce Act ("E–Sign Act")…"

- ***Specht v. Netscape Communications Corp*. 306 F.3d 17, (2nd Cir. 2002)**

ESIGN & UETA In Practice

Online terms incorporated into a written contract are valid

- ***Int'l Star Registry of Ill. v. Omnipoint Mktg., L.L.C.,* 510 F.Supp.2d 1015, 1026 (S.D.Fla.2007)**(finding that invoice referencing terms and conditions (including a forum selection clause) contained on defendant's website and signed by an officer of the plaintiff was an enforceable contract).

ESIGN & UETA In Practice

Email signature line sufficient to form contract

- ***Bazak International Corp. v. Tarrant Apparel Group,* 378 F. Supp. 2d 377 (S.D.N.Y. 2005)**(finding that the typed signature appearing on the signature line in an email was sufficient to bind the party who sent it to the terms of the email).

ESIGN & UETA In Practice

Contract terms by 'Click-Wrap' agreement are valid

- ***Metro. Reg'l Info. Sys., Inc. v. Am. Home Realty Network, Inc.*, 722 F.3d 591, 600-03 (4th Cir. 2013)** (finding that, by clicking "yes" in response to electronic terms of use agreement prior to uploading copyrighted photographs, a subscriber signed a written assignment of exclusive copyright ownership in those photographs).

ESIGN & UETA In Practice

Electronic Terms of Service are enforceable if presented to a user-signer together with a required 'Sign Up' button

- ***Fteja v. Facebook, Inc.,* 841 F.Supp.2d 829 (SDNY 2012)** (finding that consumers must be informed of terms of the transaction before signing electronically).

ESIGN & UETA In Practice

Common Hurdles:

- NOT the overall validity of electronic signatures themselves, but Issues of contract formation and substantive law:
    - Did parties AGREE to EXECUTE RECORDS ELECTRONICALLY?
    - Can we AUTHENTICATE IDENTITY of each signer?
    - Did the parties have INTENT to enter into the transaction and form a contract?
    - Did all parties have NOTICE (actual or constructive) of the transaction terms?
    - Did all parties give proper CONSENT to the terms?
    - Can we demonstrate RECORD INTEGRITY after execution?

ESIGN & UETA In Practice

Authentication may be problematic if use of account or medium through which signatures take place is not exclusive to signer

- ***Kerr v. Dillard Store Services, Inc.*, 2009 BL 30588 (D. Kan. Feb. 17, 2009)**(finding that mandatory arbitration provision in electronic agreement is unenforceable against employee because supervisor had access to employee's account and opportunity to sign employee's name).

ESIGN & UETA In Practice

Receipt of announcement email insufficient to change terms of an agreement

- ***Campbell v. Gen. Dynamics Gov't Sys. Corp*., 407 F.3d 546, 559 (1st Cir. 2005)** (finding that e-mail announcement regarding new dispute resolution policy was insufficient to put employee on notice that the policy was a contract that extinguished the right to access a judicial forum for resolution of federal employment discrimination claims).

ESIGN & UETA In Practice

Signers must have NOTICE of terms
BEFORE accepting electronically

- ***Labajo v. Best Buy,* 478 F.Supp.2d 523 (SDNY 2007)** (finding that consumers must be informed of terms of the transaction before signing electronically).

ESIGN & UETA In Practice

1. All parties must consent to working together electronically.
2. Terms being accepted must be clearly presented before execution by the parties.
3. Each party must "sign" - express its consent to the terms being presented.
4. Each party must have an exclusive and authenticated way to accept terms.
5. Each party must have ability to receive the signed record after signing.
6. Must be able to demonstrate integrity of records in storate and retrieval.

IV. Remote Notarization & eNotarization

Remote Notarization & eNotarization

eNotarization:

- Notarizing of documents electronically.
- Notary signs digitally, stamps with a digital seal, and provides a digital certificate for validation.
- Each notarization event recorded in an electronic registry.
- All other elements of a traditional, paper notarization apply to electronic notarization, including the requirement for the signer to physically appear before the notary.
- 36 states have authorized eNotarization.

Remote Notarization & eNotarization

Legal Foundation for eNotarization

- UETA – Section 11
  - If a law requires a signature or record to be notarized, acknowledged, verified, or made under oath, the 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 law, is attached to or logically associated with the signature or record.
- ESIGN – 15 U.S.C. 7001(g)
  - Adopts UETA rule for transactions in or affecting interstate or foreign commerce.

Remote Notarization & eNotarization

Legal Foundation for eNotarization

- Uniform Real Property Electronic Recording Act (URPERA) – Section 3(c)
  - A requirement that a document or a signature associated with a document be notarized, acknowledged, verified, witnessed, or made under oath is satisfied if the electronic signature of the person authorized to perform that act, and all other information required to be included, is attached to or logically associated with the document or signature. A physical or electronic image of a stamp, impression, or seal need not accompany an electronic signature
- Model Electronic Notarization Act of 2017
  - Expands provisions of the 2010 Model Notary Act

Remote Notarization & eNotarization

Remote Notarization:

- A signer personally appears before the notary at the time of the notarization using audio-visual technology over the internet instead of being physically present in the same room.

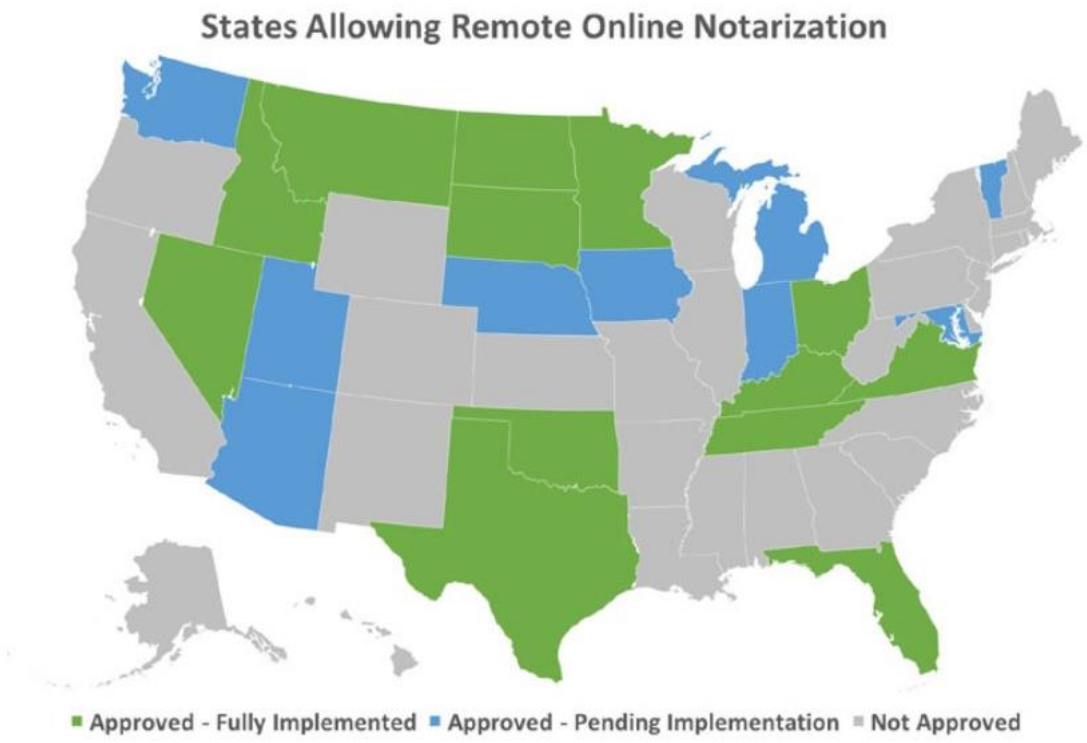
- The Remote Notarization process may involve eNotarization, but that is not a requirement.

Remote Notarization & eNotarization

Remote Notarization:

- In 2017, the Mortgage Bankers Association (**MBA**) and the American Land Title Association (**ALTA**) drafted model legislation for Remote Notarization.
- In 2018, the National Association of REALTORS® (**NAR**) enacted a policy to support adoption of Remote Notarization laws.
- In 2018, the National Association of Secretaries of State (**NASS**) officially adopted the Revised National Electronic Notarization Standards, expressly permitting the use of Remote and Electronic Notarization.
- In 2019, the Mortgage Industry Standards Maintenance Organization (**MISMO**) committed to support the model legislation drafted by ALTA and MBA.
- As of 2020, 13 states have fully-implemented Remote Notarization procedures, and an additional 9 states have Remote Notarization laws that have passed or that are entering into effect.

Remote Notarization - 2020



Source: National Notary Association (www.nationalnotary.org)

Remote Notarization & eNotarization

Legal Foundation for Remote Notarization

- No Federal solution yet.
- Remote Notarization laws are State-specific.
- Full Faith and Credit Clause of the US Constitution applies.
- Freddie Mac FAQ Statement
  - In states that permit remote electronic notarization, loans in which the borrower's electronic signature on an electronic Security Instrument or other electronic documents is remotely and electronically notarized are eligible for sale to Freddie Mac. *The notary public must be licensed and domiciled in the state in which the mortgaged premise is located and the electronic notarization law was enacted*.

V. MERS: Mortgage Industry Infrastructure Established to Support eNotes

MERS

eNotes and MERS®

- Provisions of the UETA and ESIGN ("eCommerce Laws") were intentionally drafted to enable the electronic equivalent of a promissory note, called the "eNote"
- Technical term for eNote under the eCommerce Laws is a "transferable record"
- Freddie Mac established the first practical guide for compliance with the eCommerce Law's Transferable Record rules.

MERS

eNotes

- eCommerce Laws state that an eNote created in conformity with its requirements is the functional equivalent of a paper negotiable promissory note and is just as enforceable. In addition to the requirements set forth in the eCommerce Laws on conditions to be an eNote, in order to qualify as an eNOTE, the eNote must:
  - Otherwise qualify as a negotiable promissory note under Article 3 of the UCC if it were in writing;
  - The Borrower must expressly agree that the instrument is a Transferable Record;
  - The eNote must be signed; and
  - The method use to record, register or evidence a transfer of interests in the eNote must reliably establish the identify of the person entitled to “control” the eNote
- Once these criteria are met, the person identified as the Controller obtains rights equivalent to those granted a holder of a paper promissory note, which include the right to enforce the eNote.

MERS

May "inked" paper notes be scanned and converted into transferable records?

- **Official Comment 2 to UETA Section 16:**

  "[C]onversion of a paper note issued as such would not be possible because the issuer would not be the issuer, in such a case, of an electronic record. The purpose of such a restriction is to assure that transferable records can only be created at the time of issuance by the obligor. The possibility that a paper note might be converted to an electronic record and then intentionally destroyed, and the effect of such action, was not intended to be covered by Section 16." [Emphasis added]

MERS

- MERS® eRegistry was a natural outgrowth of the MERSCORP services and with the backing of mortgage industry stakeholders became the standard for registering eNotes.

- The MERS® eRegistry is the industry standard for identifying the current Controller and location of the eNotes.

- MERS® eRegistry does not store the actual eNote but provides identifying information about it, including the eNote's digital fingerprint, the name of the Controller and the location of the eNote. The location of the eNotes themselves are stored in eVaults.

MERS

- Benefits of MERS® eRegistry:
  - eNotes are electronic and thus one copy can be identical to any other copy and no one copy can be identified as authoritative.
  - The MERS® eRegistry allows for eNotes to be registered and uniquely identified for tracking and verification.
  - Determination of the eNote's Controller and the location of the authoritative copy are determined solely by referencing the MERS® eRegistry.

MERS

MERS® eRegistry is actively tracking the ownership and the transfer of those interests in eNotes

- As of January 31, 2020:
- 499,682 eNotes registered on MERS ®
- Adoption by large originators, warehouse lenders, servicers, investors and custodians:
  - Quicken Loans (originator)
  - LoanDepot (originator)
  - Credit Suisse (Warehouse Lender)
  - Bank of America (Warehouse Lender)
  - JPMorgan Chase (Warehouse Lender)
  - PennyMac Loan Services (Servicer)
  - Fannie/Freddie (Loan Buyers)
  - US Bank N.A. (Custodian)

VI. Creating and Transferring Ownership of eNotes

CREATION AND TRANSFER - eNotes

- **Creation**: eNotes are typically created with a loan document origination system used by the originating lender. The system holds templates for various documents used in the closing process and contains the standard language used in the closing documents.

- If an eNote is created using a loan document system, the Uniform Instrument eNote Provision must be included in such note.

  - I agree that this Electronic Note will be an effective, enforceable and valid Transferable Record … and may be created, authenticated, stored, transmitted and transferred in a manner consistent with and permitted by the Transferable Records sections of UETA or E-SIGN … [T]he identity of the Note Holder and any person to whom this Electronic Note is later transferred will be recorded in a registry maintained by [Insert Name of Operator of Registry here] or in another registry to which the records are later transferred (the "Note Holder Registry"). The Authoritative Copy of this Electronic Note will be the copy identified by the Note Holder after loan closing but prior to registration in the Note Holder Registry. If this Electronic Note has been registered in the Note Holder Registry, then the authoritative copy will be the copy identified by the Note Holder of record in the Note Holder Registry or the Loan Servicer (as defined in the Security Instrument) acting at the direction of the Note Holder, as the authoritative copy.

CREATION AND TRANSFER - eNotes

- **Transfer**: As part of the closing process of the original eNote, a Mortgage Identification Number ("MIN") will be assigned and the MIN will be used to regiser the eNote with the MERS® eRegistry.

- Each transfer of an eNote is recorded in the MERS® eRegistry and a transfer will require participation from both the transferor and transferee.

- A transferor must initiate a transfer on the MERS® eRegistry and the transferee must accept such transfer.

- The transferee will then be able to specify the new location of the authoritative copy of the eNote.

VII. Post-closing: the role of the document custodian for electronic files

The Role of the Document Custodian Electronic Files

- Traditional Document Custodian is the legal fiduciary designated to administer the safekeeping of the paper promissory note.
- eNotes are custodied in a “eVault”.
- Some Controllers of eNotes use third-party services for eVaults and others maintain the eVault software in-house.
- Software solutions for eVaults are designed to maintain the identity of the authoritative copy of an eNOTE and maintain the integrity in order for it to be admissible under the Rules of Evidence.
- The ultimate responsibility for the management and integrity of the eNote rests with the party in control of the eNote.

The Role of the Document Custodian Electronic Files

- MERS® role in identifying authoritative copies:
  - eNote itself points to the MERS® eRegistry and therefore anyone reviewing any copy of the eNote is on inquiry notice that the MERS® eRegistry must be consulted.
  - When reviewing the MERS® eRegistry, anyone reviewing the entry is on notice of the location of the authoritative copy.

VIII. State Law Concerns: UCC and Recordable Instruments

E-Signatures Under the UCC

The UCC contains several of its own e-signature provisions.

- **Article 4A** covers funds transfers not covered by EFTA and does not necessarily require any written agreement, with most transfers occurring via a "commercially reasonable security procedure" (UCC 4A 202) and most other agreements relating thereto being capable of performance within 1 year.

- **Revised Article 5** permits the issuance of letters of credit as electronic records in a fashion similar to ESIGN/UETA, as well as drafts or other documents that are presented for a draw.

- **Revised Article 7** permits the issuance of documents of title as electronic records, plus in connection with ESIGN/UETA to constitute transferrable records, and further allows them to be converted to and from one medium to another medium.

E-Signatures Under the UCC

The UCC contains several of its own e-signature provisions.

- **Revised Article** 8 covers investment securities. With the exception of certificated securities, Article 8 permits securities to be evidenced and transferred via electronic means.

- **Revised Article 9** covers security interests in personal property. A security interest may attach to personal property when a security agreement becomes effective, that is, when, under UCC 9-203(b)(3)(A): "The debtor has authenticated a security agreement that provides a description of the collateral …."

- "**Authenticate**" means: (A) to sign; or (B) with present intent to adopt or accept a record, to attach to or logically associate with the record an electronic sound, symbol of process. This language mirrors ESIGN/UETA.

E-Signatures Under the UCC

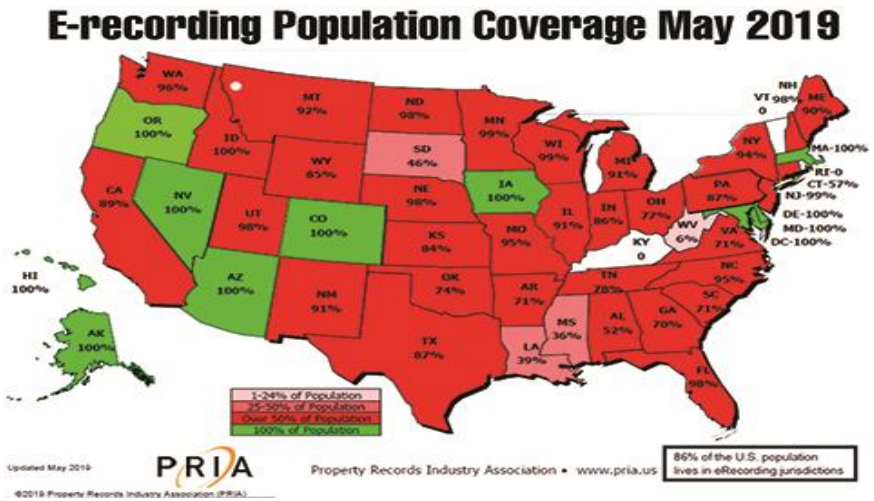
Real Estate Documentation

- A purchase agreement or mortgage is covered by ESIGN/UETA.
- ESIGN/UETA considered excluding mortgages and other real estate documents from its scope, but declined to do so.
- **HOWEVER**: to be enforceable against third parties, including a trustee in bankruptcy, a mortgage must be properly recorded in the applicable land records, which usually requires a writing, with electronic filing not available in all jurisdictions.

E-Signatures Under the UCC

Real Estate Documentation

- Almost 2,000 counties are now permitting eRecording in some form
- Over 85% of the U.S. population resides in counties where eRecording is available



E-Signatures Under the UCC

Transferable records (eNotes) as collateral? Official Comment 6 to UETA Section 16:

- "A transferable record under Section 16, while having no counterpart under Article 3 of the Uniform Commercial Code, would be an 'account,' 'general intangible,' or 'payment intangible' under Article 9 of the Uniform Commercial Code."

- "Therefore, reading the UCC and UETA together it is clear that under UCC Article 9 a secured party may perfect against electronic records (including transferable records) by filing under UCC Section 9-312(a) because electronic records constitute either accounts or general intangibles."

IX. Admissibility of Electronic Signatures and Documents Into Evidence

Admissibility of Electronic Signatures and Documents

- The Uniform Electronic Transactions Act (UETA) and the ESIGN Act each directs the admissibility of e-signatures and e-contracts into federal and state court.
- In order for an e-signature to be admissible in court, the presenter of the electronically signed contract must authenticate the e-signature by proving the intent of the signatory and the security of the signed document. It is possible that an electronically-signed document is legally valid, but inadmissible in court due to flaws in security or authentication.

Admissibility of Electronic Signatures and Documents

- In ***Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534, 538 (D.M.D. 2007),** the court summarized the evidentiary hurdles to overcome before the admission of electronic evidence:
  - 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 would otherwise be);

Admissibility of Electronic Signatures and Documents

- (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, or if not, is there admissible secondary evidence to prove the content of the ESI (Rules 1001-1008); and

Admissibility of Electronic Signatures and Documents

— (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.

Admissibility of Electronic Signatures and Documents

- **Business Records Rule, F.R.E. 803(6)**
  - **Exception to Hearsay**
  - **803(6): A record of an act, event, condition, opinion or diagnosis if:**
    - (A) the record was made at or near the time by – or from information transmitted by – someone with knowledge;
    - (B) the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling whether or not for profit;
    - (C) making the record was a regular practice of that activity;
    - (D) all these conditions are shown by the testimony of the custodian or another qualified witness, or by a certification that complies with Rule 902(11) or (12) or with a statute permitting certification; and
    - (E) the opponent does not show that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness.

Admissibility of Electronic Signatures and Documents

- Federal Rule of Evidence 901 defines how to show a document (including electronic) is authentic: "the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." **F.R.E. 901(a)**.
- As long as there is enough evidence for a reasonable juror to find that the item is genuine, the authentication threshold is met. The trial court need not be convinced that the item is authentic. It only needs to determine that a reasonable juror could find that the item is authentic.
- ESI is evaluated on a case-by-case basis for authenticity, just as any other document is analyzed. *See* ***In re F.P.*****, 878 A.2d 91, 95-96 (Pa. Sup. Ct. 2005)**.

Admissibility of Electronic Signatures and Documents

- A party is relieved from having to authenticate evidence that is produced by an adverse party, and the party that produced the evidence is a party to it or claims a benefit thereunder. *See* ***Jordan v. Calloway*, 7 So. 3d 310, 314 (Ala. 2008)**; ***Indianapolis Minority Contractors Ass'n v. Wiley*, 1998 WL 1988826, at *6 (S.D. Ind. May 13, 1998)** ("The act of production is an implicit authentication of documents produced.")
- May authenticate electronic evidence through Requests for Admission.

Admissibility of Electronic Signatures and Documents

- An easy way to use **F.R.E. 901(b)(1)** to authenticate an electronic document is to "introduce the electronic document during a deposition and have the creator or recipient of the email [or other electronic document] confirm that the email is genuine."
  - **Zachary G. Newman & Anthony Ellis, *The Reliability, Admissibility, and Power of Electronic Evidence*, AMERICAN BAR ASSOCIATION (Jan. 25, 2011)** https://apps.americanbar.org/litigation/committees/trialevidence/articles/012511-electronic-evidence.html.

Admissibility of Electronic Signatures and Documents

- **F.R.E. 901(b)** lists nine (9) examples of how items may be authenticated. This is a non-exclusive list.
- With regard to electronic evidence, the most common authentication methods are **F.R.E. 901(b)(1)** (testimony of a witness with personal knowledge) and **F.R.E. 901(b)(4)** (distinctive characteristics and the like).

Admissibility of Electronic Signatures and Documents

- **F.R.E. 901(b)(1)** allows a recipient of the email, or a non-recipient with knowledge that the communication was sent, to authenticate the email.
- The authenticating witness must establish (1) the creation of the electronic information, and (2) that the content has not been altered in any way.

Admissibility of Electronic Signatures and Documents

- Courts considering the admissibility of electronic evidence frequently have acknowledged that it may be authenticated by a witness with personal knowledge.
  - In ***State v. Bohlman*, 2006 WL 915765, at *7 (Minn. Ct. App. April 11, 2006)**, the court found a witness adequately authenticated emails she received as having come from the defendant.
  - The witness testified that the emails contained the defendant's name and email address and that she frequently sent emails to and received emails from the defendant at the email address appearing on the emails to be admitted.

Admissibility of Electronic Signatures and Documents

- An authenticating witness may be a person with general personal knowledge of how that type of document is routinely made.
- The witness must, however, provide factual specifics about the process by which the electronic document is created, acquired, maintained, and preserved without alteration, or the process by which it is produced, if it is the result of a system or process.

Admissibility of Electronic Signatures and Documents

- **F.R.E. 901(b)(4)** provides that the "appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances," may authenticate a document.

Admissibility of Electronic Signatures and Documents

- In ***United States v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir. 2000)**, the court allowed the authentication of an email entirely by circumstantial evidence, including the presence of the defendant's work email address, content of which the defendant was familiar with, use of the defendant's nickname, and testimony by witnesses that the defendant spoke to them about the subjects contained in the email.

Admissibility of Electronic Signatures and Documents

- ***United States v. Safavian*, 435 F. Supp. 2d 36, 40 (D.D.C. 2006), rev'd on other grounds, 528 F.3d 957 (D.C. Cir. 2008)**.
  - The court admitted emails (relying on FRE 901(b)(4)) based on the email addresses contained in the "to" and "from" fields, and because other identifiable matters such as the work involved, signatures, and other personal and professional references.
  - The court also permitted other emails to be authenticated under FRE 901(b)(3) by allowing the comparison of email addresses and formats to permit related emails into evidence.

Admissibility of Electronic Signatures and Documents

- Another way in which electronic evidence may be authenticated under Rule 901(b)(4) is by examining the Metadata for the evidence.
  - "**Metadata**" is information describing the history, tracking or management of an electronic document, including the date, time and identity of the creator of an electronic record, as well as changes made to the document. *See* Appendix F to *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age*
- A party may request production of ESI in its native format, which includes the metadata for the electronic document.

Admissibility of Electronic Signatures and Documents

- **F.R.E. 901(b)(9)**: Evidence describing a process or system and showing that it produces an accurate result.

Admissibility of Electronic Signatures and Documents

- ***Ruiz v. Moss Bros. Auto Grp.*, 232 Cal. App. 4th 836, 846 (Cal. Ct. App. 2014)**:
  - The appellate court upheld the trial court's finding that the defendants had not presented sufficient evidence to allow the signature's authentication.
  - The plaintiff did not recall electronically signing any documents on the day in question, and the representative could not show "that an electronic signature in the name of [plaintiff] could only have been placed on the 2011 agreement . . . by a person using [plaintiff's] unique login ID and password." *Id.* at 844.

Admissibility of Electronic Signatures and Documents

- ***Rogers v. THD At-Home Services, Inc.*, EDCV 14-02069 JGB (SPx), 2015 WL 12862912, at *4 (C.D.C.A. 2015)**.
  - The United States District Court for the Central Division of California held that Defendants had provided the court with sufficient evidence to authenticate Rogers' e-signature. There, the signature in question was authenticated by the following evidence --

Admissibility of Electronic Signatures and Documents

- Rogers conceded that he "remembers going to the site . . . and clicking on the documents that [he] was supposed to sign." However, he "do[es] not remember what documents were included there, or reading any of them." It is therefore not surprising that he does not specifically recall e-signing the Agreement.
- Second, Kathy Rodriguez-Ambriz, a Human Resources Administrator for U.S. Remodelers, explains that the company's software uses special security features to ensure that signatures could not be forged. Rodriguez-Ambriz declares that she has reviewed Rogers's application, and that his electronic signature could be generated "only if the person indicating acceptance of the agreement was logged in to the website using Brian Roger's unique login credentials."

Admissibility of Electronic Signatures and Documents

- **Best Evidence Rule, F.R.E. 1002**
  - An original writing, recording, or photograph is required in order to prove its content unless these rules or a federal statute provides otherwise.
  - An "**Original**" of a writing or recording means the writing or recording itself or any counterpart intended to have the same effect by a person who executed or issued it. For ESI, "original" means any printout – or other output readable by sight – if it accurately reflects the information.