



# eEvidence and Legal Issues



MBA Document Management & Custody Conference 2008

## eEvidence & Legal Issues

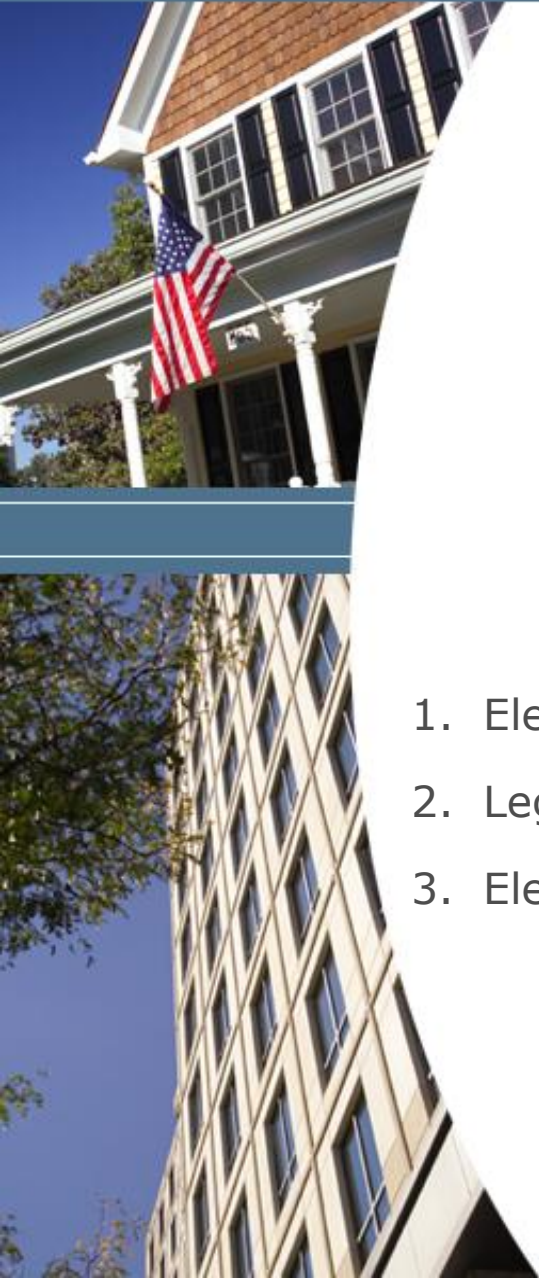
### PRESENTERS

- » Margo Tank, partner, Buckley Kolar, LLP
- » Michael Laurie, vice president & co-founder, Silanis Technology

### MODERATOR

- » Charles E. Epperson,  
Director of eBusiness, Stewart





1. Electronic transaction is more than just an electronic signature
2. Legal enforceability depends on strength of evidence
3. Electronic evidence should be easy to understand - presentation

## Uniform Electronic Transactions Act (UETA)



- State law solution
- Authorizes replacing “writings” with electronic records
- Authorizes use of electronic signatures
- Overly statute
- Adopted in 48 jurisdictions

## Electronic Signatures in Global and National Commerce Act (ESIGN)

- Federal Solution
- Instant 50 state baseline
- Provides specific requirements for consumer transactions
- Sets boundaries for regulatory authority
- Technology neutral

ESIGN and UETA give legal force and effect to “electronic signatures.”

An electronic signature is:

- An electronic sound, symbol or process
- Attached or logically associated with a contract or other record, and
- Executed or adopted by a person with the intent to sign the record

Resource



**Standards & Procedures for Electronic Records & Signatures**

<http://www.spers.org> **SPeRS<sup>SM</sup>**



Technology + (Business Processes & Procedures) = Reliable Evidence

The execution of an e-signature should be preceded by an opportunity for the signer to review:

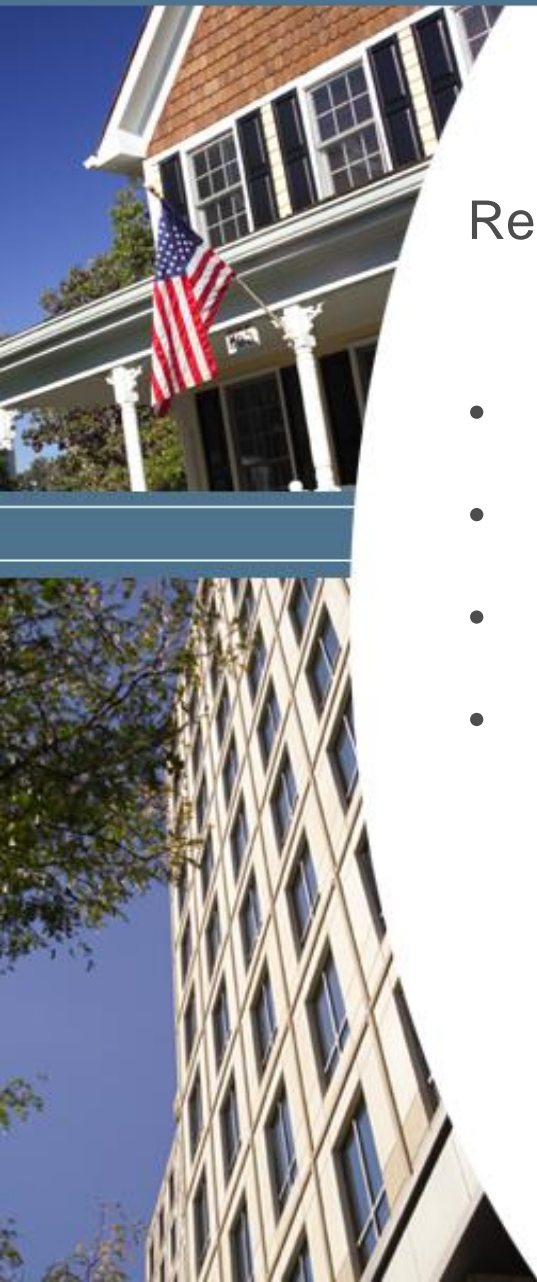
- » A description and explanation of the procedure used to create the electronic signature, and
- » A description of the sequence of events that will result in the signature becoming final and effective.

**The process used to create an e-signature should be designed so that the purpose is clear:**

- I intend to be bound
- I received the agreement or product
- I read the agreement
- I authored the record

**A process for signing records should be designed so that:**

- The record is presented for signature before the signature becomes effective, and
- The signature is attached to, or logically associated with, the record presented.
- The process surrounding creation or affirmation of the signature is preserved for the life of the transaction.



Reliable record retention system is critical for a number of reasons to:

- Enforce legal obligations
- Comply with state or federal “writing” requirements
- Meet other state or federal record retention requirements
- Obtain admission of electronic records into evidence in the event of a dispute

**ESIGN** and **UETA** focus on the accurate **preservation** of, and **access** to, the information contained in the electronic record.

In the event of a dispute the record holder must be prepared to demonstrate that the electronic record:

- » Accurately reflects the information contained in the record at the time it was signed or delivered,
- » Is accessible to anyone entitled to access the record holder's copy of the Record under an applicable rule of law or agreement,
- » Can be accurately reproduced for later reference, and
- » Is capable of being retained by transaction participants to whom it has been made available for review or signature.

**336 B.R. (9th Cir. BAP 2005)**

**11-factor foundation process for electronic records:**

- The business uses a computer.
- The computer is reliable.
- The business has developed a procedure for inserting data into the computer.
- **The procedure has built-in safeguards to ensure accuracy and identify errors.**
- The business keeps the computer in a good state of repair.
- The witness had the computer readout certain data.
- The witness used the proper procedures to obtain the readout.
- The computer was in working order at the time the witness obtained the readout.
- The witness recognizes the exhibit as the readout.
- The witness explains how he or she recognizes the readout.
- If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact. *Id.* at 14 (citing Edward J. Imwinkelried, *Evidentiary Foundations* § 4.03[2] (5th ed. 2002)).



## 241 F.R.D. 534(D. Md. 2007)

**Whenever electronic documents are offered as evidence, the party proffering the electronic information must consider the following:**



- whether the electronic evidence is relevant (Rule 501);
- the authenticity of the information (Rule 901(a));
- whether the information is hearsay, including relevant expectation, if the document is offered for its substantive truth (Rule 801);
- the original writing rule (Rules 1001-1008); and
- whether the probative value of the document is substantially outweighed by the danger of unfair prejudice or other considerations (Rule 403).

Records Retention control procedures should include:

- Control of access to databases
- Recording and logging of changes
- Backup practices
- Audit procedures
- Media deterioration
- Data migration
- Encryption of executed documents to prevent undetected alteration



TIP

**Preserve evidence: screen shots, process flows, affidavit, good witness**

*(Person v. Google; Bar-Ayal v. Time Warner; American Express v. Vin Vinhnee)*

## Types of Electronic Signatures



*Online*

Click-to-sign, typed data

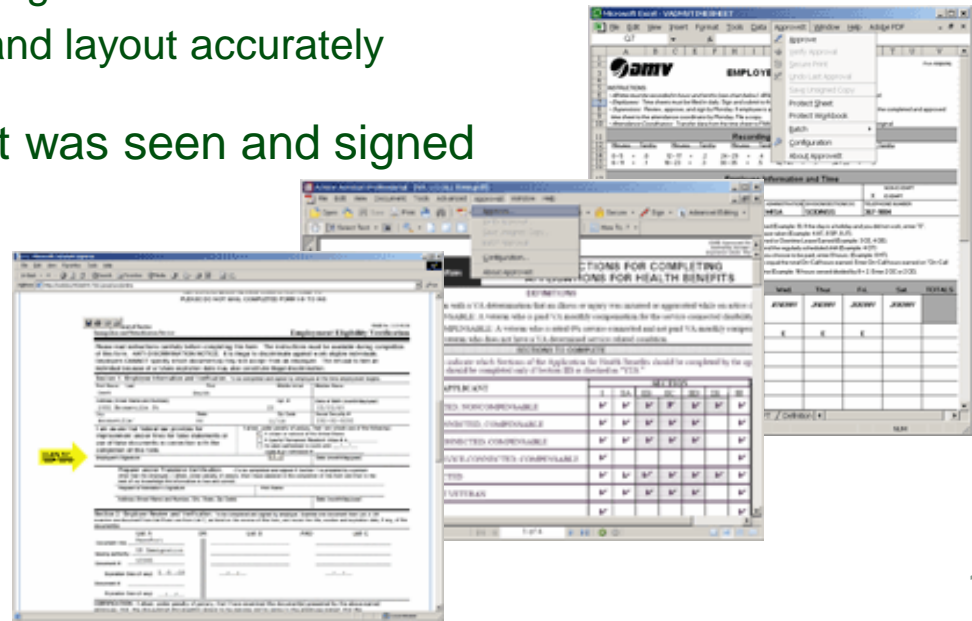


*Point of Sale*

Tablet signature input

## Document Review Process

- ☞ Screen-based – browser vs. application
- ☞ Paper-based – LCD tablet provides alternative navigation
- ☞ Affirmative act linked to signature location and document
- ☞ Present all information and layout accurately
- ☞ WYSWYS – link what was seen and signed



## *Online*

- First time* – knowledge-based authentication (internal, third-party)
- Subsequent* – user ID and password

## *Point of Sale*

- First time* – credential verification (driver's license, etc.)
- Subsequent* – credential verification or option for User ID, password

*✓ Point of Sale normally includes authentication of a representative or their system used in the signing event*

*✓ Authentication and identity data must be attached to the e-signature data for attribution*



## Electronic signature data securely linked and embedded

- ☞ Signature block + audit trail of signature event and security

## Digital signature renders e-record tamper-evident

- ☞ Retrievable and verifiable for accuracy
- ☞ Records can also be locked if practical

## Remains accessible for as long as required

- ☞ PDF is an ISO standard for e-documents

## Privacy of customer information protected

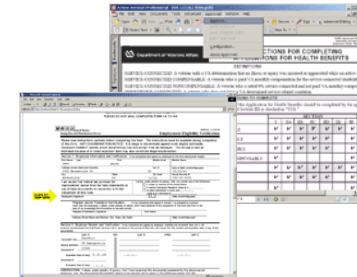
- ☞ Encrypted browser access to documents
- ☞ Secure logins to access storage of e-records
- ☞ Accesses are logged and auditable

- ☞ **Menu** driven access to transaction documents
- ☞ Blanket **consent** process to conform with ESIGN
- ☞ **Capture and store** all viewed web pages and actions by signers as evidence
- ☞ Web-based **document deliveries** are also part of electronic evidence
- ☞ Electronic evidence is **digitally signed** to be tamper-evident
- ☞ Electronic evidence is **securely linked** to e-signed records
- ☞ Secure audit trails and logs of **system accesses and actions**



CLICK TO  
SIGN HERE

\_\_\_\_\_  
Borrower's Signature: X  
Page 2 of 4 VMP-21



## Audience

- » Opposing Attorneys
- » Expert Witness/Support
- » Judge
- » Jury

## Presentation of electronic evidence

- » Electronic
- » Paper

## Affidavits

- » Authenticate electronic evidence





## Electronic records in viewable format

- ☞ Software for verifying record integrity
- ☞ Audit trail of electronic signing event

## Transaction data and records

- ☞ Audit trail of overall transaction data in presentable format

## Web session playback

- ☞ Live – network connection
- ☞ Stored - DVD, USB Memory

## Slide Presentation format

- ☞ Native, PDF, PPT, videotape



**Presentation must be clear, organized and easy to understand**



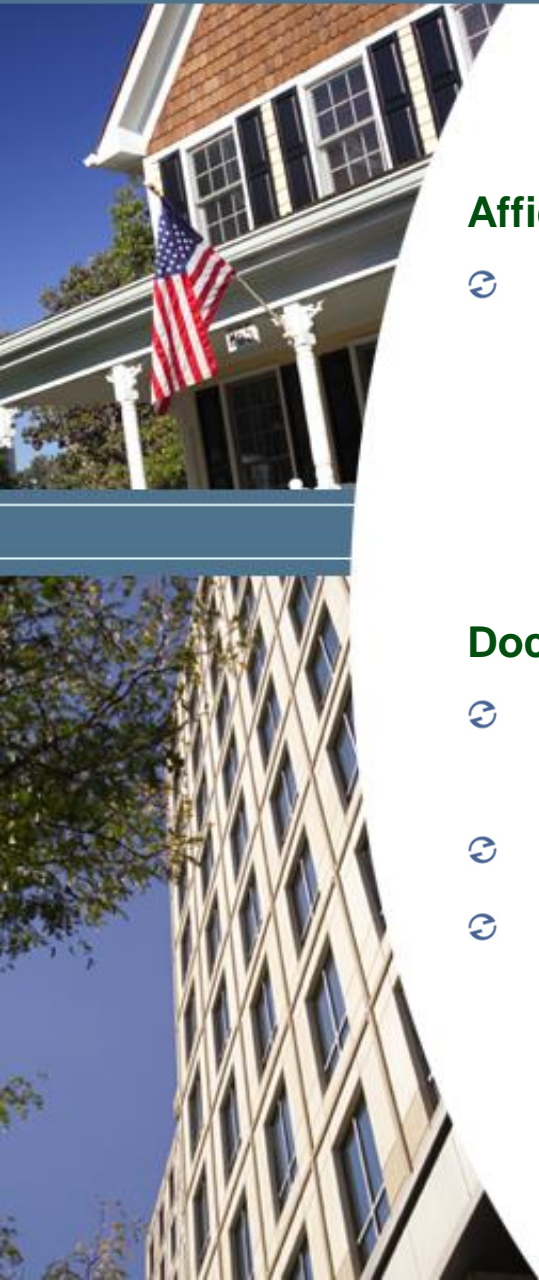
## Electronic record print-outs

- ☞ Signature block
- ☞ Audit trail for signature event
- ☞ Verification report



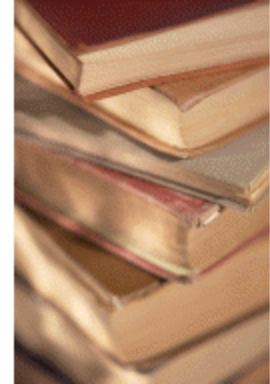
## Web-process electronic evidence print-outs

- ☞ Series of web pages viewed
- ☞ Descriptions of pages, actions and timing
- ☞ Transaction audit trail
- ☞ Documents, users, systems, timing, etc.
- ☞ Security report



## Affidavits

- ☞ Affirm the reliability and authenticity of:
  - Documents and data being presented
  - Technical processes and systems
  - Administrative procedures



## Documentation

- ☞ Standard operating procedures to prove normal business practices and exceptions
- ☞ Technical processes and systems
- ☞ Administrative procedures

QUESTIONS?

