



SPeRS

Implementing Electronic Signatures and Records: Strategies Developed by the Financial Services Industry

Electronic Financial Services Council

Jeremiah S. Buckley
Buckley Kolar LLP

jbuckley@buckleykolar.com

Legal Authority for Electronic Signatures

- Common law
 - Any mark can be a signature
 - Concern over the enforceability of electronic transactions
- Solution: Today, enforceability of electronic transactions is primarily governed by ESIGN and UETA
 - UETA – State law
 - Reported by NCCUSL in 1999
 - Adopted in 47 jurisdictions
 - ESIGN – Federal statute
 - Enacted in 2000
 - Reverse Preemption

ESIGN/UETA Are Overlay Statutes

- Legal recognition of the use of electronic records and signatures does not in any way waive the need to comply with underlying substantive law governing the transaction.
- For example, disclosures must be made at the time and in manner required by law.

Three Principles of E-SIGN/UETA

- Electronic records and signatures cannot be denied legal effect or enforceability solely because they are in electronic form
- If a law requires a record to be in writing, an electronic record satisfies the law
- If a law requires a signature, an electronic signature satisfies the law

Basic Elements of ESIGN/UETA

- Agreement/Consent to engage in business electronically
- Elements of an Electronic Signature must be met
- Record Retention (by all parties)

ESIGN or UETA – Which Law Applies?

- It is likely that both ESIGN and UETA will apply to the transaction.
- ESIGN allows state to modify, limit or supercede ESIGN:
 - By adopting the official version of UETA or
 - By adopting a state alternative that is consistent with ESIGN.
 - Many UETAs are adopted with some variance from ESIGN or NCCUSL text.

General Statute Creates Implementation Questions

- Flexibility creates a problem – You can, but how?
- Financial services industry's approach: Standards and Procedures for electronic Records and Signatures (SPeRS).

What is SPeRS?

- Cross-industry Initiative
- Behavioral Guidelines
- Rules of the road
- Technology Neutral
- Can be used to aid businesses with implementation and to assess vendors

The SPeRS Organization

- SPeRS was originally conceived by the Electronic Financial Services Council
 - Non-profit corporation
 - Sponsored by EFSC
 - Separate membership
- SPeRS Drafting Committee members – diverse points of view:
 - Corporations
 - Trade Associations
 - GSEs
 - Industry Utilities (e.g., MERS)

The SPeRS Participants

- AIG
- ACORD
- Adobe Systems
- Alliance of American Insurers
- American Financial Services Association
- American Bankers Association
- American Council of Life Insurers
- American International Group
- Bank One
- BeTrusted
- Charles Schwab
- Citicorp
- Dealertrack
- Dell Financial Services
- Esurance
- Fannie Mae
- First American Title Insurance Company
- Freddie Mac
- Genworth Financial, Inc.
- Harland Financial Solutions
- Intuit Inc.
- MassMutual Financial Group
- Mortgage Bankers Association
- MGIC
- National Association for Variable Annuities
- National Multi Housing Council
- National Notary Association
- NewRiver
- PricewaterhouseCoopers
- Principal Financial Group
- Republic Mortgage Insurance Co.
- RPost, Inc.
- Route 1 LLC
- SafeDocs, Inc.
- Securities Industry Association
- Silanis Technology
- Software & Information Industry Ass.
- SwiftView, Inc.
- Swiss Re
- TIAA-CREF
- United States Notary Association
- Verisign
- Wave Systems
- Wells Fargo Home Mortgage
- Zions Bancorporation/ Digital Signature Trust

The SPeRS Structure

- SPeRS is divided into five sections:
 - Authentication
 - Consent to use electronic records and signatures
 - Agreements, notices and disclosures
 - Electronic signatures
 - Record retention
- Each section provides 4 to 7 high-level standards to guide system design teams in developing processes that will meet the new legal requirements

The SPeRS Structure (continued)

- Each standard designed to provide insight into system design
- Each standard is supported by:
 - Plain-English discussions of the underlying issues,
 - Checklists outlining specific strategies and options for implementing the standards,
 - Examples and illustrations, and
 - Legal commentary to assist in-house counsel.

Authentication – SPeRS § 1

- Identifying and Evaluating the Appropriate Authentication Strategy – Creating the Relationship (1-1)
- Identifying and Evaluating the Appropriate Authentication Strategy – Credentials (1-2) (Credential v. Authentication)
- Providing Consumers Information Concerning the Distribution of Risk of Unauthorized Transactions (1-3)
- Establishing the Authority of Representatives (1-4)

Common Authentication Problems

- Risk of Fraud
- Allocating risk of loss
- Can/Should the credential be used by an agent?
- Balancing access and security

Consent to use Electronic Records and Signatures – SPeRS § 2

- General Agreement to Use Electronic Records & Signatures (2-1)
- Applicability of the ESIGN Consumer Consent Process (2-2)
- The ESIGN Consumer Consent Disclosures (2-3)
- The ESIGN Consumer Consent Disclosures – Format & Timing (2-4)
- Obtaining the Consumer's Affirmative Consent – Methods and Timing (2-5)
- Reasonable Demonstration of Access (2-6)

Parties Must Agree to Engage Electronically

- Agreement/Consent:
 - UETA – facts and circumstances
 - ESIGN – affirmative consent/multiple disclosures/reasonable demonstration
- Type of agreement may differ depending on
 - Type of parties (consumer/business)
 - Prior dealings (single transaction/repeat business)
 - Potential liability
 - Risk of fraud

Agreements, Notices and Disclosures – SPeRS § 3

- General Principles for Display and Presentation of Information (3-1)
- Delivering and Displaying Records and Information (3-2)
- Delivering and Displaying Records and Information – Retention of Records by Other Transaction Participants (3-3)
- Indicating Agreement (3-4)
- Acknowledging Access or Delivery (3-5)
- Clear & Conspicuous Disclosure (3-6)
- Using Hyperlinks and Other Navigational Cues (3-7)

Disclosure Issues

- Are the disclosures legally required?
- How will the disclosures be delivered?
- Ensuring that records can be retained if required
- Make the disclosures intelligible –
electronic pitfalls and opportunities
 - Pop-Ups
 - Hyperlinks

Electronic Signatures – SPeRS § 4

- Selecting a Signature Process (4-1)
- Providing Information on the Signing Process (4-2)
- Establishing the Intent to Sign (4-3)
- Associating an Electronic Signature with a Record (4-4)
- Attributing a Signature (4-5)
- Electronic Agents (4-6)

Signature Elements

- An electronic signature: any sound, symbol or process, attached to or logically associated with the contract or other record and executed or adopted by a person with the intent to sign.
- Examples:
 - Mouse Click ("I agree" button)
 - Typed name (see Shattuck v. Klotzbach (MA 2001))
 - Digital Certificate
 - PIN/Password
 - Sound
 - Biometrics (fingerprint, voiceprint)

Signature Elements (continued)

- Intent – signature (which includes the process) needs to evidence the signer's intent to be bound by the terms and conditions.
 - Can be determined by context in which signature was made (ceremony, statements made before applying signature).
- Logical Association – requires parties to have recordkeeping process that can provide evidence that a signature was applied to specific document (e.g., signature incorporated as part of record, or signature stored separately but can be associated with record later in time).

Record Retention – SPeRS § 5

- Meeting Accuracy, Accessibility and Retention requirements (5-1)
- Verifying the Integrity and Accuracy of Electronic Records/The Physical and Logical Environment (5-2)
- Verifying the Consistency and Integrity of Electronic Records (5-3)
- Document Conversion (5-4)
- Vendor Relationships (5-5)
- Interaction with Governmental Agencies (5-6)
- Transferable Records and Electronic Chattel Paper (5-7)

Record Retention is Critical

- Failure to keep adequate records can severely impact operations
 - Records are evidence – but are they admissible?
 - Hearsay rule and exceptions
 - Statements against interest
- Electronic records must:
 - Accurately reflect the information set forth in the record, and
 - Remain accessible for later reference.
- Challenges:
 - Document authenticity (letterhead, logos, other indicia of reliability)
 - Document integrity (contents sent are same as contents received; document remains intact – content can migrate due to technology advances)
 - Process Integrity

SPeRS' Flexibility Leads to Deployment in Many Areas:

- Mortgages: MISMO
- Automotive Retail Financing: ANSI X9 103-2004
- Electronic Document Storage
- Deploying electronic signature technology

Applications for ePrescriptions

- Common issues
 - Authentication/Credentials
 - Consent to prescribe electronically
 - Dealing with consumers
 - Providing important notices/disclosures
 - Security of communication
 - Ensuring adequate recordkeeping
- Requires consideration of all applicable regulations

Conclusion

- E-SIGN and UETA allow for electronic transactions, but do not provide implementation guidance
- SPeRS attempts to provide implementation guidance
- ePrescriptions may find useful tips from SPeRS' experience
- Contact:
 - EFSC: www.efscouncil.org
 - SPeRS: www.spers.org
 - jbuckley@buckleykolar.com