

Basics Workshop 2 – Key Legal Requirements for the Mortgage Industry

MBA's 2007 Legal Issues in Mortgage Technology Conference

November 27 – 29, 2007

Coronado, California

**BUCKLEY KOLAR LLP**

- ESIGN/UETA
- URPERA
- FRB Revisions to Consumer Protection Regulations
- SPeRS
- GLBA

- **State law solution for electronic records and signatures**
- **Created by the National Conference of Commissioners on Uniform State Laws (NCCUSL)**
 - **Overlay statute**
 - **48 U.S. Jurisdictions**
 - **States add non-uniform provisions**
 - **Authorizes replacing writings with electronic records**
 - **Authorizes electronic signatures**

- A Federal solution:
 - It covers state and federal laws
 - It is an instant 50 state baseline for the use of electronic signatures and records
 - It provides specific requirements for consumer transactions
 - It sets boundaries for regulatory authority
 - It is technology neutral

- The general rule of validity is that a signature, contract, or other record related to any transaction in or affecting interstate or foreign commerce may not be denied legal effect, validity, or enforceability solely because it is in electronic form.
- The admissibility of an electronic record cannot be denied solely because it is in electronic form
- E-SIGN and UETA *only affect* laws imposing writing or signing requirements and do *not* affect:
 - Substantive protections of any law, including consumer protection laws; or
 - The content, timing or format of disclosures required by law.

- ESIGN and UETA give legal force and effect to **electronic signatures**. The law defines an electronic signature as:
 - 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.
- Shattuck v. Klotzbach, 14 Mass. L. Rep. 360 (Mass. Super. Ct. Dec. 11, 2001) – Real estate contract can be formed by signed emails

- E-SIGN answers the question of “Is it a signature?”
- E-SIGN does not answer the questions:
 - “Why was the signature created?” (Purpose)
 - “Did the signer want to create and signature?” (Intent)
 - “Whose signature is it?” (Authentication)
- The recipient – not the signer – bears the burden of proof

- Limits from laws and regulations
- Characteristics of the signer
- Risk of repudiation
- Security of process
- Portability

- Consent required
 - Both UETA and ESIGN are “opt-in” statutes
 - For business-to-business transactions, and consumer transactions under UETA, consent may be
 - Express
 - Inferred from the circumstance
 - For consumer transactions under ESIGN, consent must be express in most circumstances
 - Secondary market may require retention of consent

- 3 Step Process

- Disclosures

- Assent

- Reasonable Demonstration

- Prior to obtaining a consumer's consent, the electronic record provider must deliver a clear and conspicuous statement informing the consumer of:
 - Any right or option of the consumer to have the record provided or made available in paper form;
 - The right of the consumer to withdraw consent and any conditions or consequences (which may include termination of the parties' relationship) of such a withdraw;
 - Whether the consent applies (i) only to the particular transactions which give rise to the obligation to provide the record, or (ii) to all identified categories of records that may be provided during the course of the parties' relationship;
 - The procedures the consumer must use to withdraw consent and to update information needed to contact the consumer;
 - How the consumer may after consenting, upon request, obtain a paper copy of the electronic record and whether any fee will be charged for such a copy; and
 - The hardware and software requirements for access to and retention of the electronic records.

- The consumer must consent electronically, by **reasonably demonstrating** that the consumer can access the information on the electronic form that will be used to provide the information that is the subject of the consent.

- ESIGN allows copies of contracts and state and federal disclosures to be retained electronically so long as the contract or other record:
 - Accurately reflects the information set forth in the contract or other record;
 - Remains accessible to all persons who are entitled to access by statute, regulation, or rule of law, for the period required by such statute, regulation, or rule of law in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise
- Electronic records meeting this test can satisfy “original” requirements
- Consequences for failure to retain appropriately
 - Impaired enforceability
 - May not satisfy regulatory requirements
 - May not be admissible

- Challenges:
 - Document integrity (contents sent are same as contents received; document remains intact).
 - Content prints/stores accurately.
 - Content will need to migrate due to technology advances.
 - Having a witness that can explain system

- 336 B.R. 437, 2005 Bankr. LEXIS 2602 (9th Cir. Bank. App. Panel Dec. 16, 2005)
- Admissibility of Electronic Records to Prove Amounts Owed by Debtor

1. The business uses a computer
2. The computer is reliable
3. The business has developed a procedure for inserting data into the computer
4. The procedure has built-in safeguards to ensure accuracy and identify errors

“Although this is a generally serviceable modern foundation, the fourth step warrants amplification, as it is more complex than first appears. The "built-in safeguards to ensure accuracy and identify errors" in the fourth step subsume details regarding computer policy and system control procedures, including control of access to the database, control of access to the program, recording and logging of changes, backup practices, and audit procedures to assure the continuing integrity of the records.”

5. The business keeps the computer in a good state of repair
6. The witness had the computer readout certain data
7. The witness used the proper procedures to obtain the readout
8. The computer was in working order at the time the witness obtained the readout
9. The witness recognizes the exhibit as the readout
10. The witness explains how he or she recognizes the readout
11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact

- Transferable Record (15 U.S.C. § 7021(a); UETA § 16(a))
 - Would be a note under UCC 3 if on paper
 - Issuer expressly agrees is a transferable record
 - Related to a loan secured by real property (ESIGN only)
- Possession → Control (15 U.S.C. § 7021(b)-(f); UETA § 16(b)-(f))
- Control: “a person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred”

- 6 part test
 - A single authoritative copy of the transferable record exists which is unique, identifiable and except as otherwise provided in paragraphs 4, 5, and 6, unalterable;
 - The authoritative copy identifies the person asserting control as
 - The person to which the transferable record was issued; or
 - If the authoritative copy indicates that the transferable record has been transferred, the person to which the transferable record was most recently transferred;
 - The authoritative copy is communicated to and maintained by the person asserting control or its designated custodian;
 - Copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control;
 - Each copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy; and
 - Any revision of the authoritative copy is readily identifiable as authorized or unauthorized
- Solution: MERS eRegistry + reliable Vault
- Freddie Mac eMortgage Handbook requires legal opinion that vault satisfies the safe harbor

- ESIGN and UETA already provide statutory basis for eRecording
- Approved by NCCUSL 2004
- Adopted in 15 states (AZ, AK, DE, DC, FL, ID, IL, KS, NV, NM, NC, TN, TX, VA, WI)
- Pending in 8 states (CT, MA, MN, MO, RI, SC, UT, WA)
- Overlay statute
- Does **not** require county recorders to accept electronic records
- Provides for the establishment of statewide electronic recording commission on how to implement electronic recording
- Property Records Industry Association (“PRIA”) works to provide guidance and standards

- Final Rules
- Affects FRB consumer protections regulations
 - Regulation B: Equal Credit Opportunity
 - Regulation E: Electronic Fund Transfer
 - Regulation M: Consumer Leasing
 - Regulation Z: Truth in Lending
 - Regulation DD: Truth in Savings
- Repeals interim final rules
- ESIGN Consumer Consent Process not required for Regulation Z “shopping” disclosures
- ESIGN Consumer Consent Process need not be followed if relying upon paper disclosures
- Duplicate rescission notices not required in transactions involving joint owners
- 90 day rule withdrawn

- A cross-industry initiative to establish commonly understood “rules of the road” available to all parties seeking to take advantage of the powers conferred by ESIGN and UETA
- Helps create the implementation guidance not present in ESIGN, UETA, or URPERA
- Initially published 2003
- Founded on the proposition that much of the time and effort being invested by companies “re-inventing the wheel” could be avoided if cross-industry standards for these elements of electronic transactions could be established
- Focused on the behavioral and legal aspects of the interaction between parties to the transaction, not on technology. SPeRS is intended to be technology neutral
- Standards are not necessarily legal minimums, but implementing the standards should enhance reliability and sufficiency
- Adopted by mortgage industry to develop compliant eCommerce implementations

- SPeRS is divided into five sections:
 - Authentication
 - Consent
 - Agreements, notices and disclosures
 - Electronic signatures
 - Record retention
- Each section provides 5 to 10 high-level standards to guide systems designers in developing processes that will meet the new legal requirements.
- 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.

- Increase in the number of laws applicable to the collection, use, transfer and security of personally identifiable information (GLBA, FACTA, and state laws).
- Contractual obligations (privacy promises, marketing materials)
- Governmental commitment to investigating and prosecuting violations
- Consumers educated about privacy rights

- Privacy and Security – distinct but interrelated concepts
- Privacy may be defined as the right of individuals to control the use of information about them
- Security may be defined as the safeguards utilized by businesses to protect information from unauthorized access

- GLBA requires financial institutions to disclose to all of its customers the institution's privacy policies and practices with respect to information sharing with nonaffiliated third parties.

- Your privacy policy must be an accurate description of your company's practices.
- If a company has different on-line and off-line privacy policies this should be clearly stated.
- There may be consequences if you use or transfer personal data in a manner that violates your stated privacy policy.

- Customer information clearly is a major asset and adopting a very restrictive privacy policy may effectively limit the use of a primary asset.

- GLB also requires financial institutions to establish standards relating to the administrative, technical and physical safeguarding of customer information.
- Federal Banking Agencies and the FTC have issued rules with respect to information sharing practices (16 CFR pt. 313) and safeguarding customer information (12 CFR pt. 30, 208, 211, 225, 263 and 568 and 16 CFR pt. 314)

- Federal regulators require that financial institutions implement a comprehensive written information security program to:
 - Ensure the security and confidentiality of customer information;
 - Protect against anticipated threats or hazards to the security or integrity of such information;
 - Protect against unauthorized access to or use of such information.

- What type of security measures do I really need?
- How much security is “legally” sufficient?

- Financial institutions must develop, implement and maintain a comprehensive written information security program that is appropriate to its size and complexity and the nature and scope of its activities.

- Written program should focus on:

1. oversight/accountability

FTC requires the appointment of a privacy officer – Banking agencies require oversight by the board of directors.

2. assessment of risk

identify and assess risks to customer information that could lead to unauthorized use or disclosure.

Consideration should be given to:

1. how the institution will detect, prevent and respond to attacks or system failures
2. employee training
3. the oversight of third party service providers
4. testing and monitoring measures

- Federal agencies have focused on providing a process-oriented approach to establishing security measures rather than requiring implementation of a specific standard.
- The obligation is what is reasonable under the circumstances.

- While regulators seem to be providing flexibility on one hand they also appear to be creating a “reasonable care” standard.

- Companies should:
 1. Analyze all collection, use and transfer of personal data;
 2. Institutionalize the policy;
 3. Review and revise key agreements (to among others thing limit reuse and keep information secure);
 4. Implement and test technical security measures;
 5. Conduct initial and ongoing training;
 6. Monitor the regulatory framework and implement subsequent changes.

- Web site users must have actual notice of the contents of the privacy policy
- Web site privacy policies should be presented clearly and conspicuously on the site (e.g. link to policy appear prominently on every page on which personal information is collected).
- Receipt of initial notices posted on a website must be acknowledged by the customer.

- Standards and Procedures for Electronic Records and Signatures: www.spers.org
- Electronic Signatures and Records Association: www.esignrecords.org
- Electronic Financial Services Council: www.efscouncil.org
- MERS: www.mersinc.com
- National Conference of Commissioners on Uniform State Laws (NCCUSL): www.nccusl.org
- Property Records Industry Association: www.pria.us

Margo H.K. Tank

Buckley Kolar LLP

1250 24th Street, NW

Suite 700

Washington, DC 20037

D: 202.349.8050

E: mtank@buckleykolar.com

F: 202.349.8080

www.buckleykolar.com