

# E-Discovery and Amendments to the Federal Rules of Civil Procedure

2007 Legal Issues in Mortgage Technology  
Conference

November 29, 2007

Charlotte M. Bahin, Esq. and Robert S. Gerber, Esq.

# Amendments to the Federal Rules of Civil Procedure

- **Rules 16/26:** Discovery of Electronically-stored information addressed early.
- **Rule 26(b)(2):** Data storage issues.
- **Rule 25(b)(5):** Privilege addressed early.
- **Rules 33/34:** Production method options.
- **Rule 37:** Limited safe harbor (“good faith”).
- **Rule 45:** Mirrored in Subpoena Process.

# RULE 26(b)

- Revised Rule 26(b) provides that although generally a “party need not provide discovery of electronically-stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost,” the trial court “may nonetheless order discovery from such sources if the requesting party shows good cause ...”

IMPACT: Need to prepare an Electronic Discovery Plan identifying what electronic information is “reasonably accessible” and will be produced, versus that information which is more difficult to access.

# Rule 26(b)

- Significant Change--Identify what not producing

– Responding Party must identify “**sources containing potentially responsive information that it is not searching nor producing.** The identification should, to the extent possible, **provide enough detail** to enable the requesting party to evaluate the burdens and costs of providing the discovery and the likelihood of finding responsive information on the identified sources” (Committee Notes 26(b)(2))

# Rule 26(b)

- Identification of what not producing
  - Initial response, can satisfy by listing “category or type” and burdens and costs.
- Disagreement and consequences
- Identification does not relieve preservation obligation

# Rule 26(f)

- Rule 26(f) revised to include a provision requiring that the initial disclosures and initial conference between counsel include a discussion of “any issues relating to preserving discoverable information.”
- Initial Disclosures: relevant electronic information that is reasonably accessible must be produced in due course; also provide what information is not readily accessible (26(b)(2))

# Rule 26(f) - cont

- Rule 26(f) Conference:

- Rule 26(f) requires discussion of the “disclosure of discovery of electronically stored information, including the form or forms in which it should be produced.
- To adequately prepare for this discussion, requires counsel to familiarize themselves with their client’s document retention policy and electronic storage and management systems prior to the Rule 26 Conference.

# Counsel

- Issue “Litigation Hold”
- Communicate directly with Key Players, with periodic reminders
- Instruct all employees to produce electronic copies of relevant active files
- Ensure retained data is identified and stored in a safe place
- Familiarize yourself with Local Rules and controlling case law regarding cost-shifting so, depending on whether you are the requesting party or the producing party, you can adequately gauge the potential burden on your client cost-wise in enforcing electronic discovery requests (i.e., motion/investigation costs vs. burden and costs to locate and produce)

# Company

- Identify Key Players
- Suspend document destruction
- Issue “Litigation Hold”
- Continue to recycle backup tapes? MAYBE.
  - Depends on tape use and determination of “Key Player” Information

# Tips

## Requesting Party

- Identify/Seek/Request request preferred form
- If native form requested, take precautions
- Consider narrow requests for Electronically-stored information
  - May lose cost-shifting
  - Avoid boomerang
  - Factor for determining “good cause”

# Tips

## Responding Party

- Identify preferred production form
- Objections to native form and state intent for preferred form
- Log for chain of custody to authenticate
- Prepare standard responses to standard requests
- Be prepared to provide support/software

# Authentication and Admissibility

- ***Lorraine v. Markel American Ins. Co.***, PWG-06-1893 (D. Md May 4, 2007). (101 Pages) 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).

# Foundation of E-Documents into Evidence

- **E-mails may be authenticated by a witness with personal knowledge**
  - **The authenticating witness must “provide factual specificity about the process by which the [e-mail] is created, acquired, maintained, and preserved without alteration or change or the process by which it is produced if the result of a system or process that does so.”**

# ESI and Records Management

- Absent special technology, ESI content is not tied to the medium on which it resides
- However, content may be bundled not only with medium but with policy enforcement
- Data replicates effortlessly, challenging chain of custody
- Data sent is not always received, or the same as data received
- Openness of systems / Internet
- Ease of perfect copies and of modification (photos/video/signatures/docs)
- Decentralization and distributed processing (SOA, SaaS, Virtualization)
- Improved efficiencies change definition of reasonableness

# Custodians

A custodian or other qualified witness (often) needs to testify as to the source of the information, business circumstances associated with the record's creation and the degree of regularity of the business practice and the record making and maintaining of records

- Who or what is a custodian of an e-record? (a person? a group? a function? a system?)
- What qualifications and knowledge make for reliable testimony?
- How does one deliver that e-record in a manner that can be easily authenticated?
- But what will replace the custodian?

# Sources of inaccessible records

- Technology obsolescence
- Proprietary or obsolete formats
- Legacy systems with no migration path
- Little or no systematic administrative control of records – narrow focus of risk assessment
- Inattention to record life cycle management
- Failure of senior management to establish policy and provide sufficient resources

# Importance of Policy

- Policy adopted at highest levels of company
- Policy based on electronic media
- Enterprise wide
- Policy takes regulatory requirements into account
- Training of all employees
- Compliance by all employees
- Detailed policies about specific tasks required versus general tasks required can be dangerous

