

*Electronic Discovery 2007:*  
**A Primer for Financial Institutions**

---

*Changes to the  
Federal Rules  
of Civil Procedure*

THE **SANTA FE** GROUP  
A Publication of The Santa Fe Group Vendor Council  
April 2007

### *About The Santa Fe Group Vendor Council*

The Santa Fe Group Vendor Council promotes the development of secure, best-in-class technology solutions, standards, and improved business processes for the financial services industry and beyond.

Our interactive and strategic approach bridges the disconnect between vendors and the corporate user community. Through meetings, workshops and other events, Vendor Council members gain unique opportunities to interact with industry leaders and fellow members on critical technology issues, concerns and solutions. For more information about The Santa Fe Group Vendor Council, please contact Robin Slade, senior vice president, at 630-653-9340 or [robin@santa-fe-group.com](mailto:robin@santa-fe-group.com).

### *About The Santa Fe Group*

The Santa Fe Group is a strategic consulting company providing expertise to financial institutions and other critical infrastructure companies. Drawing from the most advanced thinking in the industry, access to a wide network of business, technology and security experts, and a deep knowledge of regulatory and legislative issues, The Santa Fe Group brings outstanding results to its clients. The Santa Fe Group is a strategic partner and preferred provider to BITS, the nation's foremost authority on technology and financial services. For more information, visit us on the web at [www.santa-fe-group.com](http://www.santa-fe-group.com) or write to us at [info@santa-fe-group.com](mailto:info@santa-fe-group.com).

## *I. Purpose of the New Rules*

On December 1, 2006, changes to the Federal Rules of Civil Procedure took effect in all federal courts in the US, formalizing procedures and expectations for electronic discovery.

Changes to the FRCP affect every business involved in federal litigation. While complex, the new rules provide much-needed clarity for electronic discovery processes. They provide opportunities to save time and money, reduce business disruption, make information systems more efficient, and provide safe harbor for the well-prepared.

The new rules seek to address a number of problems and ambiguities with electronic information discovery, including:

- The significant costs and burdens of producing electronic discovery
- A lack of clarity as to how parties should handle e-discovery logistics
- The challenge of reviewing often enormous volumes of electronic documents for privilege before they are produced to the opposing party
- Inconsistencies that allow legal gamesmanship such as oversupplying or hiding evidence, or providing electronic discovery in a degraded format

The changes:

- Accelerate the rate of exchange of information between parties
- Clarify logistics for discovery planning and execution
- Help parties provide appropriate responses to e-discovery requests
- Reduce opportunities for gamesmanship
- Establish clear rules for dealing with privileged electronic information

## *II. Explanation of the Rules*

Each company will need to review the new rules individually and in their entirety with counsel to determine how the rules may affect them. This section summarizes the key points of the changes that are most likely to be of relevance to financial institutions and other large, information-intensive organizations.

### **1. Initial meeting to discuss e-discovery**

To help parties address e-discovery issues early in the litigation process, changes to rules 26 and 16 require parties to meet at the start of litigation to discuss document preservation. The idea is to balance preservation with the need to continue routine business operations.

The parties should:

- Discuss where relevant information resides and its accessibility
- Identify the person or persons with special knowledge of the producing party's computer system
- Identify the subject of the e-discovery and time frame to produce
- Identify the sources of information that are within a party's control and subject to discovery, and whether that information is reasonably accessible, taking into account the burden and cost of retrieving and reviewing the information

To appropriately address these issues, companies need to identify and communicate with appropriate IT staff, such as network administrators, email administrators, database specialists and data backup experts. These individuals will play a critical role in the litigation as information experts during discovery, and may testify about information availability, particularly if there is a dispute between the parties.

The "meet and confer" process includes a discussion of claims of privilege or work product protection. The parties may decide to agree on procedures for asserting claims after information is produced.<sup>1</sup>

## **2. Defining e-discovery, determining accessibility, and forms of production**

In the past there was inconsistency among various courts as to what was considered an electronic record. For example, judicial interpretations varied with respect to whether instant messages or spreadsheet formulas were considered records. Revised Rule 26 ends individual interpretation and establishes electronically stored information (ESI) as a separate category of information subject to production, encompassing data and information of all kinds stored on any medium from which it can be retrieved and examined.

The “reasonable accessibility” of a data source depends on whether responding to the request would cause “undue burden or cost” to the responding party. Possible data sources falling into this category are:

- Legacy data from antiquated computer systems
- Data stored on backup tapes
- “Deleted” data that may still exist, but in fragmented form

The burden falls on the producing party to provide sufficient detail on information it asserts is not reasonably accessible. In many cases IT staff will be needed to determine the information’s location, age, encryption, and other relevant attributes.

Rule 34(b) permits a requesting party to specify the form in which it would like the ESI to be produced. The idea here is to make clear preferred forms of production and prevent the producing party from disadvantaging the requesting party by downgrading the format of the information. If the parties do not agree on the form of production, the responding party must produce the information in the form in which it is ordinarily maintained.<sup>2</sup>

### **3. Preservation of privilege and the possibility of waiver**

Electronic information volumes are vastly greater than traditional paper volumes. Rule 26(b)(5)(B) responds to the practical difficulty or impossibility of pre-reviewing for privilege electronic information that must be produced.

To ease this burden, the rules allow parties to decide on one of two procedures relating to privilege and work product protection during the meet and confer process: the “clawback” and the “quick peek.” With a “clawback,” the parties agree that privileged documents inadvertently produced will be returned upon request. In a “quick peek,” the producing party allows the requesting party to look at its documents prior to any privilege review and then request what it wants to be produced. The producing party is always expected to show that it took reasonable measures to screen the information for privilege prior to production. IT experts are critically important in this process of sorting through data and identifying pertinent material for attorneys.

When privileged information or work product materials are produced, the producing party must notify the receiving party that it is claiming privilege or protection of the electronic information, making clear the basis for the claim. If there is a disagreement, the receiving party may request a ruling as to whether the information is in fact protected or privileged.

#### **4. The scope of discovery**

Rule 26(b)(2)(B) addresses ESI that cannot be reviewed without expensive retrieval and restoration, based on undue burden and expense.

“Inaccessible information” is considered presumptively non-discoverable and does not have to be produced unless the requesting party shows “good cause” for requiring the information. A producing party does have to identify the sources it claims are inaccessible. “Reasonably accessible information” that is relevant and non-privileged is presumptively discoverable.<sup>3</sup>

The term “inaccessible” is defined functionally rather than by identifying specific sources. If a requesting party challenges the assertion, the producing party has the burden of demonstrating that a source is inaccessible. If the producing party succeeds, the court may still require that the inaccessible source be searched if the requesting party can demonstrate “good cause.” In determining good cause the court must consider factors including: “(1) the specificity of the discovery request, (2) the quantity of information available from more readily available sources; (3) the failure to produce information that for some reason is no longer available but one suspects should have been; (4) the likelihood of finding responsive information that cannot be obtained from a more readily available source; (5) predictions as to the importance and usefulness of the requested information; (6) the importance of the issues at stake in the litigation; and (7) the parties resources.”

If a court orders production from inaccessible sources, it may specify cost shifting or cost sharing among the parties.

## 5. “Safe harbor” provisions

The concept of “safe harbor” holds that a company does not have to halt its normal business operations because a lawsuit has been filed. The new Rule 37(f) acknowledges that businesses must routinely delete and destroy information for operating reasons and prohibits a court from imposing sanctions for failing to provide electronic information lost as a result of the routine, good-faith operation of computer systems.

In evaluating “good faith,” a court may consider whether a party intervened (for example, with a litigation hold) to modify or suspend its routine operation to prevent loss of relevant data. The obligation to preserve may arise from the common law, statutes, regulations or a court order. Only when litigation is reasonably anticipated does the obligation to intervene and suspend the routine operation of the system arise.

Attorneys should engage corporate IT managers to ensure preservation obligations are met early in the litigation. Good faith preservation may extend, for example, to information that the company does not believe to be “reasonably accessible.”

### *III. Engaging the Enterprise*

Effective information management — while always complex — can bring significant rewards to a company, both during litigation and in its everyday operations. Thoughtful, thorough and clear electronic storage, retrieval and disposal processes that take into account the diverse needs of business units and the company’s duty to respond quickly to information requests can yield substantial cost savings and efficiencies.

The following recommendations can help companies to best manage electronic information. Together, they form the basis of an effective enterprise-wide ESI policy.

- 1. Create a litigation team.** The team should include representatives from legal, IT, records management and compliance, and should establish electronic information systems, processes and oversight.
- 2. Formalize record retention policies.** Policies should include system implementation and schedules, ensuring that the electronic records retention process is consistent with paper processes. Implement education and training.

**3. Formalize document preservation and hold policies.** Have a system for logging information put on hold, a database of what is on hold and what is released, and an internal communication plan that includes messaging models.

**4. Document information destruction processes.** Well documented processes for destroying data are critical to supporting claims of safe harbor.

**5. Create a map of your electronic information.** The map should identify where all information resides and its attributes, how easily it can be accessed and in what format, how long it will take to produce and any implications of producing it.

**6. Identify an expert.** This person should understand corporate information processes and structure as well as legal issues, so that he or she can represent the company during the meet and confer conference.

**7. Practice “good faith.”** Treat your e-discovery program as you would a compliance program. Protect your company and your data by following clear, well documented policies, procedures and controls with appropriate implementation and oversight.

By being prepared, organizations can reduce their risk of revealing privileged material, take better advantage of safe harbor provisions, reduce disruption at their business caused by litigation, and gain better control of the valuable information they hold. Though the prospect of reviewing and improving information management practices can be daunting, the new Federal Rules of Civil Procedure present a strong rationale for the highest levels of the business to examine, renew and improve strategies for electronic information management.

1. See Section 3 for details on privileged information.
2. If that form is not usable, the information must be delivered in “reasonably usable” form.
3. This provision is subject to “the proportionality rule,” which limits discovery when “the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties’ resources, the importance of the issues at stake and the importance of the proposed discovery in resolving the issues.”

## Acknowledgements

The Santa Fe Group Vendor Council thanks the following members companies for their contributions to this paper.

**Iron Mountain Incorporated** helps organizations around the world reduce the costs and risks associated with information protection and storage. Iron Mountain offers comprehensive records management, data protection, and information destruction solutions along with the expertise and experience to address complex information challenges such as rising storage costs, litigation, regulatory compliance and disaster recovery.

**Symantec** is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries.