

Tuesday, May 31, 2005

Litigation Update - Beware Of The Potential Penalties Associated With Electronic Discovery

By Amy Abdo and Sherida Colvin

Now, more than ever, in this fast paced electronic age, companies must be aware of the potential land mine of judicial penalties lurking in their networks. While e-mail and other electronic information systems generally make your company more efficient and profitable, unless immediate precautions and procedures are implemented to preserve and manage information stored in your company's network, your company could face a severe penalty.

On May 16, 2005, a Florida jury issued a verdict against investment bank Morgan Stanley for \$604 million in damages to be paid to financier Ronald Perelman. Unfortunately for Morgan Stanley, the bad news did not stop there. On May 18, 2005, the same jury ordered Morgan Stanley to pay \$850 million in punitive damages for a total \$1.45 billion judgment. To make matters worse, Morgan Stanley may have been able to avoid this record-breaking judgment had it understood and implemented a comprehensive electronic data retention and storage policy accompanied by a reasoned strategy to respond to requests for electronic information.

The lawsuit alleged that Morgan Stanley, in its role as Sunbeam's investment banker, committed fraud by disguising Sunbeam's troubled finances, which eventually rendered Mr. Perelman's shares in Sunbeam worthless. During the discovery phase, Morgan Stanley faced fairly straightforward requests to produce e-mails and other electronic evidence. After more than ten months of inconsistent disclosure by Morgan Stanley, the Court specifically ordered it to conduct a word-search of its back-up tapes for e-mails from 36 relevant employees. To ensure Morgan Stanley's compliance, the Court also ordered it to submit an official certification that its obligations under the Order had been satisfied. Morgan Stanley disclosed e-mails and filed a certification signed by one of its executives. Following the disclosure, it became known that Morgan Stanley failed to search all of its back-up tapes to uncover e-mails specifically addressed in the Order. Many back-up tapes were subsequently discovered at numerous office locations under the control of various employees.

As a result of Morgan Stanley's failure to comply with the Court's Order, the Court imposed the extreme penalty of an "adverse inference" against Morgan Stanley. This "adverse inference" reversed the burden of proof and required Morgan Stanley to prove that it was not at fault. The Court also included in its penalty a statement to the jury that because of Morgan Stanley's misconduct and obstructionist behavior in withholding relevant e-mail evidence, it could conclude that Morgan Stanley committed fraud. Following trial, the jury returned a verdict against Morgan Stanley for \$604 million and imposed punitive damages of \$850 million.

The Morgan Stanley case highlights the importance of electronic data retention, storage, and production policies. Given the prevalence of electronic discovery in modern litigation, businesses must be able to readily access relevant evidence

quick links

- [All PDF Updates](#)
- [Litigation Attorneys](#)
- [Litigation Practice](#)
- [Contact Us](#)
- [Acrobat Reader](#)

Phoenix
3003 N. Central Ave.
Suite 2600
Phoenix, AZ 85012-2913
(602) 916-5000

Tucson
One S. Church Ave.
Suite 1000
Tucson, AZ 85701-1627
(520) 879-6800

Nogales
1891 N. Mastick Way
Suite A
Nogales, AZ 85621-1081
(520) 761-4215

Lincoln
1221 N Street
Suite 801
Lincoln, NE 68508-2028
(402) 323-6200

located on their networks, company computers and back-up tapes. It is undeniable that our courts' expectations are continuing to rise with electronic discovery. Courts expect companies to have a well-reasoned step-by-step approach to respond to requests for electronic information. Likewise, courts expect companies to be diligent to ensure full compliance with court rules and judicial orders. Should a company fail to fully comply with electronic data requests, potential sanctions include, among others, litigation costs, attorneys' fees, adverse inference instructions, striking an answer and entering default judgment, and dismissal of claims or defenses.

Here are some practical tips to ensure your company does not find itself on the receiving end of what could be devastating sanctions:

Preserve Evidence - Companies need to be aware of the easily triggered duty to preserve evidence whether in hard copy or electronic form. The duty to preserve arises once litigation is reasonably foreseeable. To satisfy this duty, affirmative measures must be taken to protect evidence that (i) is potentially relevant to a matter; or (ii) you should anticipate will be requested during litigation. This duty includes preserving e-mail or other electronically stored information as well as electronic information that has been "deleted" but is still retrievable. In the face of a duty to preserve, the company should consider suspending standard practices of deleting and destroying information, and recycling electronic storage space. The excuse that relevant information is no longer available due to the company's destruction or recycling practices, will not shield the company from sanctions.

Review Policies - Assuming relevant evidence has been destroyed pursuant to company policy or practice, in determining whether sanctions are warranted, courts will examine the company's reasoning and goals behind the policy. The company should be prepared to prove that (i) the policy or practice is reasonable given the facts and circumstances; (ii) it has not been faced with frequent lawsuits or complaints; and (iii) the company implemented the policy or practice for legitimate business reasons. In the face of a potential claim, the failure to halt destruction policies or practices may be viewed as bad faith. Cross-reference your document destruction or preservation policies and practices with corporate compliance policies to ensure consistency.

Develop a Plan of Attack - Whether a party to litigation or the recipient of a third party subpoena, companies need to be in a position to readily locate, access and preserve information. If you are not a party to a lawsuit, yet are served with a subpoena, the production may be due in less than thirty days. To ensure timely compliance and avoid a potential crisis, the plan of attack must be in place. Company management and counsel should work together to develop a plan that can be followed on short notice. The plan should include an analysis of the scope of the request and a mechanism to ensure comprehensive preservation techniques. For example, this could include immediately taking hard drives out of service that were used by key witnesses until a forensic mirror image can be made. Many computer users do not recognize that the continued use of any computer system may result in the loss of critical evidence. The plan must include a comprehensive search of available electronic systems as well as discontinued databases or back-up tapes. Additionally, the plan should ensure all necessary employees are on notice of the duty to preserve evidence. They should be given steps to follow to preserve and identify potentially relevant information. The plan also should address suspension of the company's retention, destruction and recycling policies or practices.

Educate Outside Counsel - Be certain that outside counsel understands your network, including parameters for retention of information, how electronic information is stored, the costs associated with retrieval and restoring information, company policies that apply to electronic information, how the policies were developed and implemented, and company practices associated therewith.

Develop a Response Team - To ensure compliance, it takes a concerted team effort by the client, counsel and Information Systems (IS) personnel. Include senior IS personnel in the drafting and implementation of retention or destruction policies that deal with electronic evidence. Appoint a senior member of the IS Department (IS Representative) to oversee and take responsibility for handling requests for electronic evidence. Be selective! The appointed representative may become a key witness to your defense.

Provide Necessary Training - Ensure IS personnel are sufficiently trained to deal with electronic evidence and that they understand the manner in which evidence is stored and/or automatically deleted from the company's network. Educate all IS personnel about "unknown" or "hidden" areas for storage of electronic evidence, including, without limitation,

unallocated disk space, deleted files and back-up tapes. Provide continued training to your IS personnel so they remain abreast of technological advances. If the company updates, improves or changes its electronic systems, determine to what extent existing data will continue to be accessible. Ensure the IS Representative is familiar with the information that may no longer be accessible through the new system and that it may be accessed by other means.

Instruct Employees on Retention and Destruction Policies - Employees should know and understand company policy on retention and destruction of information. Ensure employees understand the policy applies to electronic information, the purpose of the policy, means to comply with the policy, and potential risks if the policy is not followed. Instruct employees on organizational techniques to utilize in storing electronic information. This will ensure a more thorough and efficient response to requests for information. Do not let untrained employees search for responsive information. Instead, it should be the responsibility of the IS Representative or closely supervised and trained staff. If IS personnel must have access to key employees' computer systems, provide access at times that will minimize inconvenience to key employees.

Outline Scope of Request - Review the request for information with counsel and the IS Representative to identify (i) date parameters; (ii) geographic parameters; (iii) individuals involved; (iv) whether deleted files must be recovered, restored and produced; (v) whether back-up tapes must be searched; (vi) the form in which the data must be produced; and (vii) whether an outside consultant would facilitate a more efficient, effective and economical response. Finally, consider data versus meta-data. Meta-data is data about data. For example, it reveals information about a document's history, including, among others, authors, creation date, modification dates, access dates, and print dates. Meta-data has become useful in settling factual disputes or testing a witness's memory. Make sure your review methods capture and include meta-data where appropriate.

Keep a Log of all Responsive Activities - From the day the duty to preserve arises to receipt of the request to the actual production, the appointed IS Representative should keep a detailed log of all steps taken to ensure the company has searched for, located, preserved, identified and produced all responsive information. The detailed log will be key evidence in proving to a court that you responded in good faith by (i) performing a diligent and thorough search; and (ii) following a well-reasoned plan of attack. Be extremely thorough in your review of the network and back-up tapes in an effort to avoid a court-ordered intrusion into your information systems.

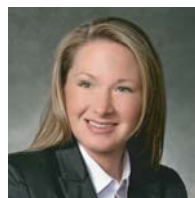
Establish a Review Protocol - After all of the responsive information is gathered, establish a review protocol designed to be sensitive to issues of privilege and responsiveness.

Maintain Corporate History and Knowledge - If the appointed IS Representative leaves the company, it is important to capture his or her corporate knowledge and pass it on to a successor. Keep the corporate history with the company regarding, among other information, dates and manner of changing or upgrading electronic systems, storage of electronic information, and location of back-up tapes, so that you are not faced with a lack of corporate knowledge when responding to a request for electronic information.

Electronic discovery is highly fact specific. The circumstances of each case or request for information will dictate an appropriate course of action. If your company takes adequate measures prior to an obligation to preserve or produce electronic information, when the time comes, you will be well prepared to avoid insurmountable challenges and potentially devastating penalties.



Amy Abdo
Director
602.916.5399
amy@fclaw.com



Sherida Colvin
Associate
602.916.5417
scolvin@fclaw.com