Franchise Valuations LIMITED SM

Franchise Technology Risk Management

The Franchise Valuations Reporter

404 Park Avenue South, 16th Floor, NY, NY 10016
O: 212.689.0400 / Bruce@FranchiseValuations.com

Volume 2, Issue 3 – March 2010

Our areas of expertise in the franchise, distribution and dealership context are:
Finance, accounting and tax;
Damages, valuations and expert testimony; and
Cyber-security and E-discovery of ESI (Electronically Stored Information)
We offer a free initial consultation. If any readers have questions, you are welcome to email or phone us and we will provide our best answer as quickly as possible.

Bruce S. Schaeffer, Editor
Bruce@FTRM.biz

If you do not want to receive this email reporter you may unsubscribe below.

ESI and E-Discovery: *Zubulake* Revisited

In December, 2006, revisions to the Federal Rules of Civil Procedure, particularly Rule 26, governing discovery of Electronically Stored Information (ESI) – commonly known as E-discovery – went into effect. Judge Shira A. Scheindlin of the Southern District of New York is generally recognized as the foremost authority on the consequences of failure to comply with E-discovery rules based on a series of decisions she rendered starting in 2004, generally referred to as the *Zubulake* decisions, which were the foundation for the Federal Rules changes. In January, 2010, Judge Scheindlin returned to the issues in *Pension Committee v. Banc of America Securities*, and sub-titled the opinion "*Zubulake* Revisited: Six Years Later."

Using no-nonsense and entertaining language, she delivered a clear message: a casual, do-it-yourself, approach to implementing litigation holds or conducting cursory searches will not cut it. (at p. 84) "While litigants are not required to execute document production with absolute precision, at a minimum they must ask diligently and search thoroughly at the time they reasonably anticipate litigation." The import of the decision is clear – delay the search (or conduct it in a lame fashion) and you will be subject to sanctions.

Sanctions even without intentional spoliation

In *Zubulake* Revisited, Judge Scheindlin wrote, "This case does not present any egregious examples of litigants purposefully destroying evidence." Nonetheless, she found that the actions and inactions of 13 of the plaintiffs constituted negligence and/or gross negligence and imposed sanctions – some very severe.

Practitioners should take particular note of four failures she cited as sufficient to find **gross negligence**:

1. Lack of **timeliness of written litigation hold** (p. 63): "I have already held that . . . the failure to issue a written litigation hold in a timely manner amounts to gross negligence."

- Litigators must be aware that, at least since 2007, a litigation hold requires more than just a say-so. It requires input, action and supervision from computer knowledgeable experts.

2. Failure to include **all relevant parties** (including current and former employees) in the search parameters and the litigation hold, to insure that their electronic and paper records are preserved. Judge Sheindlin held it was gross negligence to know that backup tapes existed but elect not to search them – or to fail to extend the searches to personal computers or palm pilots (or Blackberrys, iPhones etc.).

- Litigators must be aware that identifying relevant parties and devices to be searched requires a combined effort by lawyers and computer knowledgeable experts.

3. Failure to "**preserve backup tapes** when they are the sole source of relevant information or relate to key players." (p. 59) For example, one sanctioned litigant in its purported litigation hold failed to alter its document retention policy so the recycling of backup tapes continued and discoverable information continued to be overwritten.

- Litigators must be aware that a direction to preserve ESI must be more than a piece of paper; it requires specific instructions, in a combined effort by lawyers and computer knowledgeable experts, to insure that all ESI is preserved.

4. **Inadequate supervision** and oversight in the document search and production process. (p. 49) In the case of one plaintiff, the job was delegated to a person with no experience conducting searches of ESI who received no specific instruction, no supervision, and had no contact with counsel. She, in turn, delegated some searches to others.

- Litigators must be aware that sending just anyone to compile and review ESI is no longer adequate. The decisions make it very clear – the compilation and review must be conducted by knowledgeable people with computer expertise.

Call in the experts

It's time to face up to the fact that most lawyers and their clients are simply not equipped to deal with the details and technical aspects of ESI and E-discovery. In the view of Magistrate Judge John M. Facciola of the U.S. District Court in Washington, D.C., "Electronic discovery is now too technical and complex for attorneys to assess adequately, and . . . experts may be necessary to determine whether an e-discovery search is adequate." (Quoted in "Rockin' Out the E-Law," ABA Journal, July 2008.)

Practitioners should be aware that our technology division, Franchise Technology Risk Management (FTRM), provides experts in electronically stored information (ESI) and computer security coupled with decades of experience in franchising.

Choice of sanctions available to court

E-discovery must be handled correctly or a litigant will be made to hurt all over. In the words of Judge Scheindlin, "Parties need to anticipate and undertake document preservation with the most serious and thorough care, if for no other reason than to avoid the detour of sanctions." (p. 25). The penalties for failure to conduct proper e-discovery include, in order of severity:

Ordering of further discovery
Cost-shifting
Fines
Special jury instructions
Preclusion
Entry of default judgment or dismissal

Get FTRM involved early to avoid pitfalls

FTRM can help litigants avoid costly mistakes in every stage of the litigation process:

- examination of retention policies and storage policies;
- design and implementation of litigation holds;
- advice on whether or not to image hard drives (or to demand such action from an adversary);
- designing search strategies and key word criteria for all media;
- participating in pre-trial discovery conferences; and
- proper production of relevant data.

As Judge Sheindlin noted, good intentions in the face of technical ignorance will not be tolerated. She noted that a "pure heart and empty head" are simply no defense (at p. 8) and that sanctions will result when the facts "have demonstrated that [litigants] conducted discovery in an ignorant and indifferent fashion." (at p. 81)

Daubert Decisions – Damages Experts

Two recent cases are instructive to show where *Daubert* challenges will fail. In *Arlington Industries v. Bridgeport Fittings*, 2009 WL 2973472 (USDC PA September 10, 2009) which involved patents rather than franchises the defendant claimed that the expert 1) misapplied the legal standard; 2) was not a technical expert with respect to the market for the particular patented product; and 3) failed to supply a proper foundation for his report. But the court dismissed the challenge and made short shrift of the "not a technical expert" argument by saying "Frankly, given the relative frequency with which accountants are permitted to offer lost profits testimony in infringement suits . . . the defendant's arguments are anemic".

However, in *Lock Realty Corp. v. U.S. Health, LP*, 2009 WL 2970330 (USDC IN September 14, 2009) the expert was precluded even though she was a CPA and a credentialed business appraiser with more than 20 years experience.

In that case, the court found the expert's analysis used none of the three traditional approaches to valuation (cost, income and market) but rather relied on an email from the defendants and a Medicaid calculation of

fair rental value. The court further noted that the expert's analysis did not provide the source data and figures by which another expert could replicate her work holding, "An expert must offer good reason to think that her approach produces an accurate estimate using professional methods, and this estimate must be testable. Nothing in the record suggests that the plaintiff's expert relied on generally accepted methods used for valuing property and her opinion cannot be tested for accuracy." (emphasis added) Thus her report and testimony were inadmissible.

Nexus Notes

"Physical Presence" Not a Requirement for Sales Tax Nexus – Proposed Statutory Presumption in California

Another so-called "Amazon" bill has been introduced in the CA legislature that would provide that a dealer is presumed for retail sales and use tax purposes to be soliciting or transacting business in the state by an independent contractor, agent, or other representative if the dealer enters into an agreement with a state resident under which the resident, for a commission or other consideration, directly or indirectly refers potential customers, whether by a link on an Internet site or otherwise, to the dealer.

Democrats in the CA legislature think a levy on retailers such as Amazon and Overstock.com could bring in up to $150 million annually. As reported by the *Los Angeles Times*:

"Now California is one of several cash-strapped states exploring a novel legal strategy that could force Amazon and others like it, including Overstock.com, to start collecting tax from their customers. New York launched the effort with a law that took effect in 2008. North Carolina and Rhode Island have passed similar laws; other proposals have advanced in the statehouses of Virginia, Illinois, Colorado and Hawaii."

CyberCrime

This is a terribly serious problem that most franchise systems have been so far unwilling to address. One of the most recent catastrophes – still in progress - should drive franchise practitioners to call us for secure and confidential penetration testing. As reported by the *Wall Street Journal* (2/16/10):

Hackers in Europe and China successfully broke into computers at nearly 2,500 companies and government agencies over the last 18 months in a coordinated global attack that exposed vast amounts of personal and corporate secrets to theft, according to a computer-security company that discovered the breach. . .

The damage from the latest cyberattack is still being assessed, and affected companies are still being notified. But data compiled by NetWitness, the closely held firm that discovered the breaches, showed that hackers gained access to a wide array of

data at 2,411 companies, from credit-card transactions to intellectual property. . .
The hacking operation, the latest of several major hacks that have raised alarms for companies and government officials, is still running and it isn't clear to what extent it has been contained, NetWitness said. Also unclear is the full amount of data stolen and how it was used. . .
Starting in late 2008, hackers operating a command center in Germany got into corporate networks by enticing employees to click on contaminated Web sites, email attachments or ads purporting to clean up viruses, NetWitness found . . .
In more than 100 cases, the hackers gained access to corporate servers that store large quantities of business data, such as company files, databases and email. . .
At one company, the hackers gained access to a corporate server used for processing online credit-card payments. At others, stolen passwords provided access to computers used to store and swap proprietary corporate documents, presentations, contracts and even upcoming versions of software products, NetWitness said.

How to protect yourself:

Computer users should always be wary of opening attachments or clicking on links in unsolicited e-mails and instant messages from people they don't know. With this new threat, however, even messages from familiar senders may be suspect. Make sure your antivirus and security software are up to date. Also, a Web Application firewall will help defend against certain types of attacks better than your normal firewall. Use the latest versions of operating systems and application software and be diligent about installing patches. Never give out personal information in e-mail, ever.

For those of you doing business on Facebook and other social networking sites, this is a wake-up call. If you have not implemented cyber security policies and training in your organization, you need to start now. We invite you to contact us to learn more about your risks and how to protect yourself.
To arrange a free test of your system, including a review of your web traffic logs, call us at 212.689.0400 or e-mail: Henry@FTRM.biz or Henfree@FTRM.biz.

MORE REASONS TO BE FRIGHTENED!
Links to Recent Articles on Cyber-Crime

Survey Finds Growing Fear of Cyberattacks

Hacking for Fun and Profit in China's Underworld

Swiss Banks Achilles Heel Is Workers Selling Data

Germany Weighs Buying Swiss Bank Data

Broad New Hacking Attack Detected: Global Offensive Snagged Corporate, Personal Data at nearly 2,500 Companies; Operation Is Still Running