

MARCH 30, 2012 |

Legal Developments in Securities Law

Preserving Electronic Data in a Securities Case

by: Magdalena M. Kadziolka, Esq.

Due to the nature of business in the 21st century, often some of the most important discovery in a securities case is electronic discovery.

Electronically stored information, or ESI, is often discoverable in securities litigation. The Federal Rules of Civil Procedure define ESI as information created, manipulated, communicated, stored, and best utilized in digital form, requiring the use of computer hardware and software. This can include e-mails, word processing documents, spreadsheets, metadata, pictures, text and chat messages, video and audio files, web browsing history, programming information, and many other files. At the first sign of potential litigation, a company or individual should immediately suspend all routine document retention/destruction policies in order to ensure that they meet their obligation to put in a “litigation hold.”

Recently, in New York, the Appellate Division adopted the federal decision in the seminal electronic discovery case of *Zubulake v. UBS Warburg*, 220 F.R.D. 212 (S.D.N.Y. 2003). The court in *Voom HD*

Holdings LLC v. EchoStar Satellite LLC, 2012 WL 265833 (Jan. 31, 2012) relied on *Zubulake*'s standard for preservation, and found that the Defendant in the matter demonstrated at the very least gross negligence and even bad faith by failing to apply a litigation hold until four months after an action had been commenced against it. Although this may sound like an extreme case, it highlighted the importance of preserving electronic data early in the proceedings to avoid the consequences in court.

Preservation of electronic information can be costly, but the consequences for "spoliation" of evidence may be even costlier.

Spoliation is defined by Black's Law Dictionary as, "The destruction of evidence...The destruction, or significant and meaningful alteration of a document or instrument." In *Voom*, the court applied an adverse inference charge in favor of the plaintiff for spoliation of evidence, but the court could have applied the penalty of a default judgment, the most severe sanction for spoliation. Parties may also be prohibited from supporting or opposing claims based on spoliated evidence.

Spoliation of evidence may take many forms – failing to preserve electronic data is one form, but altering documents certainly counts too.

In some cases, evidence may be inadvertently spoliated, such as if an individual accesses a file and then saves it under a new name, that may be considered spoliation of evidence in some courts as metadata and other information that could be important may have been deleted (this may depend on whether the original source has remained intact and available to the opposing party).

Of course, although the SEC has specific recordkeeping requirements that must be followed for certain entities or individuals, a company or individual should take immediate steps at the first sign of potential litigation – whether they receive a demand letter, a phone call alluding to potential violations or if a company or individuals hints that they “will sue.”

Many large companies will have specific procedures in place to follow to initiate a litigation hold. For those companies that do not, it is important to consider implementing a plan to ensure smooth preservation of all potentially discoverable material.

A potential litigant must immediately stop all document destruction – whether there is an e-mail setting that deletes e-mails after a certain period of time or a company policy in place. Electronic discovery and even saving electronic data can be very costly, but a potential litigant is not required to save every single document it possesses. Federal case law demonstrates that a litigant is required to preserve “what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request.” *See Danis v. USN Communs., Inc.*, 2000 U.S. Dist. LEXIS 16900 (N.D. Ill. Oct. 20, 2000). This duty applies to all electronically stored information, whether e-mails or other forms of files which are stored electronically, which may even include backup computers, hard drives and other computer storage media, archives and even old computers.

Limiting the scope of which documents are preserved (rather than saving 3 years of all electronic data), requires time and effort spent to determine who has knowledge of the facts in the case, which custodians (individual accounts) are relevant, when the alleged wrongdoing occurred and where all relevant documents can be found (a lot of electronic discovery may be e-mails, but other files may be relevant too). The largest expense will likely be e-mail, as the volume of the number of e-mails a particular custodian receives in only one day could be quite large. If the potential discovery involves e-mails which have already been removed and backed up in a less accessible medium, the party may be able to argue that the information is not reasonably accessible and would result in undue burden or cost to the litigant to retrieve. The court may balance this with the importance of the potential discovery, and may even provide its own parameters for a search.

In a securities case, depending on the type of case, it may be important to preserve all press releases and their drafts, financial data that in any way relates to the security at issue and all financial statements for a company or individual who is the potential litigant, e-mails which refer to the security at issue or which support any public statements made about a particular security, e-mails with individuals concerning the particular security, trading data, internal securities policies within a company, e-mails among employees who may have been involved in wrongdoing concerning the security, and many other documents that could be relevant to your case. In fraud cases, the plaintiff will be trying to establish scienter and a misstatement or omission, among other elements – e-mails will likely be helpful along with the misstatement or

omission itself, and any supporting documentation the opposing party may have. The SEC will often request the above documents, and social media documentation has become relevant lately – ensure that document preservation efforts include Facebook, Twitter, LinkedIn and any other social media accounts associated with the company and/or individuals involved. The same applies for instant messaging, G-mail chat and text messaging, all of which may be requested in an investigation, especially one involving insider trading (after all, a tip could come in any form). The bottom line is that the first step in litigation is preservation – given the potential consequences and the cost of retrieving electronic data, potential litigants can't afford to wait.