The Metropolitan
Corporate Counsel®

www.metrocorpcounsel.com

Volume 15, No. 12 December 2007

Global & Domestic Compliance Readiness – Law Firms

Getting ESI Evidence Admitted: *Lorraine v. Markel American Insurance Co.*

Jeffrey L. Nagel

GIBBONS P.C.

Introduction

Much has been written about a company's obligation to preserve, produce, and even restore electronically stored information ("ESI"), but much less has been written about the ways in which ESI can actually be used as evidence to prove one's case or defend against a charge. That is changing, as shown by the recent case of *Lorraine v. Markel American Insurance Co*., 241 F.R.D. 534 (D.Md. May 4, 2007).

On May 17, 2004, plaintiff's yacht was damaged by lightning while anchored in the Chesapeake Bay. An arbitrator found that lightning was the cause of the damage, but limited the award to $14,100. Plaintiff brought a federal action to enforce the arbitrator's finding but to set aside the limits placed on the award, claiming the arbitrator exceeded his authority. Defendant/ Counter-Plaintiff Markel American Insurance Company counterclaimed to enforce the arbitrator's award (including its damage limitation) in full.

Jeffrey L. Nagel

The problem for both sides was that neither supplied the evidentiary foundation needed for the court to rely upon various e-mails and other ESI offered in support of and in opposition to the arbitrator's award. The Court thus took the opportunity to discuss how ESI should be proffered in admissible form so it can be relied upon. As the Court stated: "Given the pervasiveness today of electronically prepared and stored records … counsel must be prepared to recognize and appropriately deal with the evidentiary issues associated with the admissibility of electronically generated and stored evidence." 241 F.R.D. at 537. "[C]onsidering the significant costs associated with discovery of ESI, it makes little sense to go to all the bother and expense to get electronic information only to have it excluded from evidence … because the proponent cannot lay a sufficient foundation to get it admitted." *Id*. at 538.

Lorraine details a number of evidentiary rules that must be considered when ESI is proffered, including: (1) whether the ESI is relevant (Federal Rule of Evidence 401); (2) whether the ESI is authentic (Rule 901); (3) whether the ESI is hearsay and, if so, whether it meets an applicable exception (Rules 801, 803, 804 and 807); (4) whether the ESI is an original or acceptable duplicate (or "best evidence") or meets an exception (Rules 1001 through 1008); and (5) whether the probative value of the ESI is outweighed by unfair prejudice (Rule 403). *Id*.

Space limitations prevent discussing every evidentiary problem examined in *Lorraine*, so this summary focuses on two concerns: authentication and hearsay.

ESI Authentication

Relevance is usually easy to demonstrate. But to be admissible, ESI must also be authentic. Authentication insures that evidence is trustworthy. ESI raises unique authentication issues, as the data can easily be altered after creation. *See Manual for Complex Litigation* at § 11.447. ("Computerized data, however, raise unique issues concerning accuracy and authenticity. Accuracy may be impaired by incomplete data entry, mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment malfunctions. The integrity of data may also be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling.")

One of the easiest ways to authenticate ESI is to obtain "[t]estimony that a matter is what it is claimed to be." *See* Fed. R. Evid. 901(b). Courts considering the admissibility of electronic evidence fre-

***Jeffrey L. Nagel** is a senior member of the Gibbons Electronic Discovery Task Force and advises clients on document retention and E-Discovery best practices. He is a Director in Gibbons' Business & Commercial Litigation Department, the Securities Litigation Team and the Private Equity and Hedge Fund Group. His practice involves the strategic planning, management, trial and appeal phases of complex litigation, as well as arbitration. Mr. Nagel has successfully represented public and private companies and their management in litigation involving a range of corporate governance, securities and competition issues, including claims involving partnership disputes, hedge fund issues, breach of contract, fiduciary duty, fraud, and malpractice claims. He can be reached at (212) 613-2061.*

quently use this method. *See*, *e.g*., *United States v. Kassimu*, 188 Fed. Appx. 264, 2006 WL 1880335 (5th Cir. 2006) (computer records authenticated by witness with personal knowledge). It is necessary, however, that the authenticating witness provide factual specificity about the process by which the ESI was created, obtained, and preserved without alteration or change.

Federal Rules of Evidence 901(b)(3) and (b)(4) also provide common ways to authenticate ESI. Rule 901(b)(3) permits authentication by "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." 901(b)(4) allows authentication essentially through "circumstantial evidence." *See United States v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (authentication of e-mail by circumstantial evidence such as the presence of defendant's work e-mail address and use of the defendant's nickname in the e-mail).

Certain identifying marks or data contained with ESI may also allow for identification. Two common examples are "hash values" and "metadata." A hash value is a unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file. Hash values can be inserted into original electronic documents when they are created to provide them with distinctive characteristics that will permit their authentication under Rule 901(b)(4). *Id*. *See also* United States District Court for the District of Maryland, *Suggested Protocol for Discovery of Electronically Stored Information*, *available at* www.mdd.uscourts.gov/news/news/ESIProtocol.pdf (encouraging parties to discuss hash values when producing electronic records in discovery to facilitate later authentication).

Metadata is another method of establishing authenticity, since such information can provide information about a particular data set by describing how, when, and by whom it was collected, created, accessed, or modified. Because metadata shows the date, time, and identity of the creator of an electronic record, as well as all changes made to it, metadata is another distinctive characteristic of electronic evidence that can be used to authenticate under Rule 901(b)(4).

There are, of course, a multitude of additional ways to authenticate ESI, including relying on any "self-authenticating" characteristics of the ESI. As *Lorraine* notes, counsel must be "creative in identifying methods of authenticating electronic evidence when the facts support a conclusion that the evidence is reliable, accurate, and authentic, regardless of whether there is a particular example in Rules 901 and 902 that neatly fits." 241 F.R.D. at 553. The bottom line is that counsel must be ready to utilize the ESI they believe supports their client's position by making sure that such evidence can be authenticated as a first step towards having a court rely upon it.

ESI Hearsay Issues

Hearsay issues also are pervasive when ESI is introduced. Federal Rules of Evidence 801 through 807 deal with the concept of hearsay and its many exceptions, all of which cannot be addressed here. But two broad points should be made.

First, much ESI is not hearsay at all. For example, when an electronically generated record is entirely the product of the functioning of a computerized system or process – such as a "fax report" generated by the machine showing the number to which the fax was sent and the time it was received – there is no "person" involved in the creation of the record, and no "assertion" being made, so the record is not hearsay. *Id*. at 564-65; *see also State v. Dunn*, 7 S.W.3d 427, 432 (Mo. Ct. App. 2000) (Computer generated telephone records "are not the counterpart of a statement by a human declarant" and "should not be treated as hearsay."). Moreover, in many instances assertive statements are not hearsay because they are not offered to prove the truth of the assertions, for example: (1) statements offered to prove that they were false or misleading, as in a fraud or misrepresentation case; (2) statements offered to prove that certain listeners had notice of the information; (3) statements offered as circumstantial evidence of the declarant's state of mind or motive.

Second, assuming the ESI in question is "hearsay," there are a multitude of exceptions that might apply. One of the most common exceptions is the "business record exception" under Rule 803(6). The foundational elements for a business record are that: "(1) the document must have been prepared in the normal course of business; (2) it must have been made at or near the time of the event it records; [and] (3) it must be based on the personal knowledge of the entrant or of an informant who had a business duty to transmit the information to the entrant." *Lorraine*, 241 F.R.D. at 571. To have been made "in the normal course of business" means that the record was made in the course of a regularly conducted business activity, for which it was the regular practice of the business to maintain a memorandum. *Id*.

Because many employees use work computers for personal correspondence, as well as for business reasons, some care must be taken to analyze whether the common "business record exception" is applicable to ESI, especially when that ESI is an e-mail. E-mail chains present especially peculiar problems, since some courts demand that when the source of the information related in the e-mail is someone other than the maker of the e-mail, the source, the maker, "as well as every other participant in the chain" must be shown to have been acting "in the regular course of business." *State of New York, v. Microsoft*, 2001 U.S. Dist. LEXIS 7683 at *14 (D.D.C. Apr. 12, 2002). This can be an onerous standard. As *Lorraine* noted, the "lesson to be taken from these cases is that some courts will require the proponent of electronic business records or e-mail evidence to make an enhanced showing in addition to meeting each element of the business records exception. These courts are concerned that the information generated for use in litigation may have been altered, changed or manipulated after its initial input, or that the programs and procedures used to create and maintain the records are not reliable or accurate." *Lorraine*, 241 F.R.D. at 574.

Conclusion

As the use of ESI becomes more and more prevalent, so too will the application of the rules of evidence to such information. Even if ESI has cleared the authentication and hearsay hurdles discussed above, additional evidentiary rules will also apply, such as showing the material is an "original" and is not unfairly prejudicial such that it should be excluded from evidence. Today's practitioner must therefore be familiar not simply with the process of preserving, maintaining, and producing ESI, but also the evidentiary rules likely to apply to that ESI. Knowing these rules in advance and bearing them in mind at the early stages of gathering and producing ESI can be the difference between having your or your adversary's evidence admitted or excluded by the court.