

## EVIDENTIARY PROBLEMS AND ESI

Kevin F. Brady

On May 14, 2007, Chief Magistrate Judge Paul Grimm of the District of Maryland issued a 101-page opinion in *Lorraine v. Markel American Ins. Co.*, 2007 WL 1300739 (D. Md. May 4, 2007), which sets forth in definitive fashion and in great detail, the evidentiary pitfalls and solutions associated with ESI.

### BACKGROUND OF THE CASE

The case involved cross-motions for summary judgment to enforce/modify the decision of a private arbitrator decision under § 9 of the Federal Arbitration Act, 9 U.S.C. § 1 et seq. (2006) concerning lightning damage to a yacht. Because neither party complied with the requirements of Rule 56, Judge Grimm dismissed both motions without prejudice. The focus of the dispute had to do with the language of the arbitration agreement and while Judge Grimm found that the agreement was ambiguous, he could not look to the documentary evidence provided by the parties (which is what a judge would normally do) because there was admissibility problems with the evidence presented by the parties. In particular, none of the documentary evidence which consisted of the arbitration agreement, the arbitrator's award and copies of email correspondence between counsel (ostensibly submitted as extrinsic evidence for the parties' intent regarding the arbitration agreement) was authenticated by affidavit or otherwise as required by Rule 56. The Judge noted that while there has been a great deal of information distributed about what to do with electronic information before litigation and during discovery, very little has been written, however, about what is required to insure that ESI obtained during discovery is admissible into evidence at trial. With his decision in *Lorraine*, Judge Grimm has certainly filled that void.

### RECENT AMENDMENTS AND ADMISSIBILITY ISSUES

The December 2006 amendments to the Federal Rules of Civil Procedure relating to electronic information focused on the problems and potential solutions for handling ESI in discovery. But two topics were missing in the amendments: (i) how should companies deal with pre-litigation preservation issues; and (ii) how should lawyers manage ESI in order to address the unique problems associated with getting ESI into evidence. There has been a great deal of guidance regarding how to handle ESI before and after the December amendments came into effect but there has been a dearth of guidance as to how to handle

authenticity, admissibility, hearsay and other evidentiary problems associated with ESI. What is required to insure that ESI obtained during discovery is admissible at trial? What constitutes “such facts as would be admissible in evidence” for use in summary judgment practice under FRCP 56(e)?

## SUMMARY JUDGMENT MOTIONS AND EVIDENTIARY ISSUES

Judge Grimm noted that while it is well established that unsworn, unauthenticated documents cannot be considered by the Court on a motion for summary judgment because the Court may only consider evidence that would be admissible at trial. Judge Grimm then said that “considering 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 or rejected from consideration during summary judgment because the proponent cannot lay a sufficient foundation to get it admitted.” Moreover, the Judge noted that the process is complicated by the multiple faces of ESI -- e-mail, website ESI, internet postings, digital photographs, and computer-generated documents and data files.

## EVIDENTIARY HURDLES TO BE CLEARED

In *Lorraine*, Judge Grimm discusses in great detail the “collection of evidence rules that present themselves like a series of hurdles to be cleared by the proponent of the evidence. Failure to clear any of these evidentiary hurdles means that the evidence will not be admissible.” Whenever ESI is offered as evidence, either at trial or in summary judgment, the following evidence rules must be considered: (1) is the ESI **relevant** as determined by Rules 401, 402 and 105 (does it have any tendency to make some fact that is of consequence to the litigation more or less probable than it otherwise would be); (2) if relevant under 401, is it **authentic** as required by Rules 901 and 902 (can the proponent show that the ESI is what it purports to be); (3) if the ESI is offered for its substantive truth, is it **hearsay** as defined by Rule 801, and if so, is it covered by an applicable exception (Rules 803, 804 and 807); (4) is the form of the ESI that is being offered as evidence an **original** or **duplicate** under the original writing rule, or if not, is there admissible secondary evidence to prove the content of the ESI (Rules 1001-1008); and (5) is the probative value of the ESI substantially outweighed by the danger of **unfair prejudice** or one of the other factors identified by Rule 403. While Judge Grimm went into great detail in discussing each of these topics, due to space limitations, I will only discuss the issues associated with relevancy and authenticity and I refer the reader to Judge Grimm’s decision for an excellent discussion of those topics.

## PRELIMINARY EVIDENTIARY RULINGS

Before any of the five hurdles is cleared, however, Judge Grimm noted that there is an interesting interplay regarding “preliminary rulings” on admissibility (Rule 104(a) and (b)) that must be addressed. While the Court makes a preliminary determination regarding the admissibility of evidence under Rule 104(a), the Federal Rules of Evidence, except for privilege, do not apply. So the Court can and does consider hearsay or other non-admissible evidence that would not be offered to the jury when the Court decides preliminary admissibility issues. Because authentication is a subset of relevancy and “evidence cannot have a tendency to make the existence of a disputed fact more or less likely if the evidence is not what its proponent claims, ...[r]esolution of whether evidence is authentic calls for a factual determination by the jury and admissibility, therefore, is governed by the procedure set forth in FRE 104(b).”

Moreover, while courts have recognized that authentication of ESI may require greater scrutiny than that required for the authentication of “hard copy” documents, they have been quick to reject calls to abandon the existing rules of evidence when doing so. In *In Re Vee Vinhnee*, 336 B.R. 437 (9<sup>th</sup> Cir. BAP (Cal.) 2005, the court addressed the authentication of electronically stored business records. It observed “[a]uthenticating a paperless electronic record, in principle, poses the same issue as for a paper record, the only difference being the format in which the record is maintained . . . .” However, it quickly noted “[t]he paperless electronic record involves a difference in the format of the record that presents more complicated variations on the authentication problem than for paper records. Ultimately, however, it all boils down to the same question of assurance that the record is what it purports to be.” *Id.* At \*445

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. The proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy. The judge should therefore consider the accuracy and reliability of computerized evidence, including any necessary discovery during pretrial proceedings, so that challenges to the evidence are not made for the first time at trial.

Judge Grimm noted that while there is no single approach to authentication that will work in all instances, it is possible to identify certain authentication issues that the courts and the commentators have identified with particular types of evidence such as email, Internet Web postings, Instant Messaging, and computer stored records and data.

## E-MAIL

Email presents an especially interesting evidentiary challenge because there are so many ways in which e-mail evidence may be authenticated. Judge Grimm listed the most frequent ways to authenticate e-mail evidence: (i) 901(b)(1) (person with personal knowledge); (ii) 901(b)(3) (expert testimony or comparison with authenticated exemplar); (iii) 901(b)(4) (distinctive characteristics, including circumstantial evidence); (iv) 902(7) (trade inscriptions); and (v) 902(11) (certified copies of business record).

By way of example, Judge Grimm pointed out that “[p]rintouts of e-mail messages ordinarily bear the sender’s e-mail address, providing circumstantial evidence that the message was transmitted by the person identified in the e-mail address. In responding to an e-mail message, the person receiving the message may transmit the reply using the computer’s reply function, which automatically routes the message to the address from which the original message came. Use of the reply function indicates that the reply message was sent to the sender’s listed e-mail address.

Under Rule 902(7), e-mails may even be self-authenticating if there are labels or tags affixed in the course of business. For example, “business e-mails often contain information showing the origin of the transmission and identifying the employer-company. The identification marker alone may be sufficient to authenticate an e-mail under Rule 902(7). However, the sending address in an e-mail message is not conclusive, since e-mail messages can be sent by persons other than the named sender.” Because of the potential for unauthorized transmission of e-mail messages, authentication needs to also comply with Rule 901(b)(1) which requires testimony from a person with personal knowledge of the transmission or receipt to ensure its trustworthiness.

## INTERNET WEBSITE POSTINGS, TEXT MESSAGING AND CHAT ROOM CONTENT

In addressing the evidentiary problems associated with internet websites, the authentication rules most likely to apply, singly or in combination, are 901(b) (1) (witness with personal knowledge) 901(b)(3) (expert testimony) 901(b) (4) (distinctive characteristics), 901(b)(7) (public records), 901(b)(9) (system or process capable of producing a reliable result), and 902(5) (official publications). Many of the same foundational issues found encountered when authenticating website evidence apply equally to text messaging and chat room content. However, because chat room messages are posted by third parties who use “screen names,” it cannot be assumed that the content in question was posted with the knowledge or authority of the website host. Obviously, there are foundational requirements that must be

met in order to authenticate chat room evidence and the rules most likely to be used to authenticate chat room and text messages are 901(b)(1) (witness with personal knowledge) and 901(b)(4) (circumstantial evidence of distinctive characteristics).

## COMPUTER STORED RECORDS AND DATA

Given the current business practice to store massive amounts of data on computers, this can be a major source of authentication problems in particular, because as Judge Grimm noted, there is a great disparity between the most lenient approaches and the most demanding approaches. Judge Grimm identified the Court's decision in *In Re Vee Vinhnee*, 336 B.R. 437, 444 (B.A.P. 9<sup>th</sup> 2005) as the "high water mark" for demanding approaches.

The primary authenticity issue in the context of business records, as identified by the Court in *In Re Vee Vinhnee*, is "on what has, or may have, happened to the record in the interval between when it was placed in the files and the time of trial. In other words, the record being proffered must be shown to continue to be an accurate representation of the record that originally was created . . . . Hence, the focus is not on the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created." *Lorraine* \*46. The *Vee Vinhnee* Court went on to state that, for electronic information, "the logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the database are logged or recorded, as well as the structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database, are pertinent to the question of whether records have been changed since their creation." *Id.* Judge Grimm then noted that in order to meet the heightened demands for authenticating electronic business records, the *Vee Vinhnee* Court adopted, with some modification, an eleven-step foundation proposed by Professor Edward Imwinkelried:

1. The business uses a computer.
2. The computer is reliable.
3. The business has developed a procedure for inserting data into the computer.
4. The procedure has built-in safeguards to ensure accuracy and identify errors.
5. The business keeps the computer in a good state of repair.
6. The witness had the computer readout certain data.
7. The witness used the proper procedures to obtain the readout.

8. The computer was in working order at the time the witness obtained the readout.
9. The witness recognizes the exhibit as the readout.
10. The witness explains how he or she recognizes the readout.
11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.

*Id.* at 446-47 (citation omitted).

Thus, the methods of authentication most likely to be appropriate for computerized records are 901(b)(1) (witness with personal knowledge), 901(b)(3) (expert testimony), 901(b)(4) (distinctive characteristics), and 901(b)(9) (system or process capable of producing a reliable result).

### **PRACTICAL TIPS FOR ADDRESSING ESI EVIDENTIARY ISSUES**

- It is critically important that counsel be prepared to establish the authenticity and admissibility of their exhibits and that they begin to think about admissibility and authentication issues at the early stages of discovery;
- If it is critical to the success of your case to admit into evidence ESI, it would be prudent to plan, as early as possible, to authenticate the ESI by the most rigorous standard that may be applied.;
- During pretrial discovery, counsel should determine whether opposing counsel will object to admissibility of critical information. This could be accomplished by stipulation or the use of Rule 36 Requests for Admission;
- It is important for counsel to be prepared to provide the Court with enough information to understand the technology issues as they relate to the reliability of the evidence at hand; and
- Counsel need to be creative and consider whether there are case management tools that might assist the Court and the parties in addressing
- evidentiary problems concerning some of the more complex issues (such as “dynamic” data in a database or what is a “true and accurate copy” of ESI).

## ABOUT THE AUTHOR

Kevin F. Brady is a partner in the firm's Business Law Group. Kevin is a member of the firm's Hiring Committee and the Practice Leader of the Electronic Discovery and Records Management Group.

He represents clients in a variety of areas including corporate litigation, commercial litigation, electronic discovery and records management, insurance litigation and arbitration and mediation.

He is experienced as lead counsel or co-counsel on significant matters in the Delaware Court of Chancery, the Delaware Superior Court and the District of Delaware as well as multiple jurisdictions outside of Delaware.

Kevin has been recognized by Best Lawyers in America as a recommended practitioner in Delaware.

Kevin Brady can be reached at (302) 888-6257 or [kbrady@cblh.com](mailto:kbrady@cblh.com)