

Contributing Authors

Patrick J. Hatfield
phatfield@lordbissell.com
404.870.4643

Jon A. Neiditz
jneiditz@lordbissell.com
404.870.4684

Jay G. Safer
jsafer@lordbissell.com
212.812.8305

www.lordbissell.com

This *Client Alert* is provided solely for educational and informational purposes. It is not intended to constitute legal advice or to create an attorney-client relationship. Readers should obtain legal advice specific to their enterprise and circumstances in connection with each of the topics addressed.

If you would like to be removed from our mailing list, please contact us at unsubscribe@lordbissell.com or Lord, Bissell & Brook LLP, 111 South Wacker Dr., Chicago, Illinois 60606 Attention: Marketing. If we are not so advised, you will continue to receive *Client Alerts*.

Attorney Advertising

© 2007 Lord, Bissell & Brook LLP.

From E-Discovery To E-Admissibility? *Lorraine v. Markel* And What May Follow

The recent decision in *Lorraine v. Markel American Insurance Company*, 2007 WL 1300739 (DMD May 4, 2007) by United States Magistrate Judge Paul W. Grimm is an excellent guide to an important aspect of the care that MAY be or become necessary when parties attempt to offer electronic information in evidence. In that case, involving contract interpretation issues, Magistrate Judge Grimm refused to allow either party to offer e-mails in evidence to support their summary judgment motions. He found they failed to meet any of the standards for admission under the Federal Rules of Evidence. The emails were not authenticated but simply attached to the parties' motions as exhibits, as has been a common practice. This alert summarizes Judge Grimm's opinion, and then discusses briefly where it may lead e-contract and other e-document management programs.

Little could the owner or insurer of the pleasure boat *Chessie* have known that the lightning that struck *Chessie* while it rested at anchor would ultimately ignite a 101-page opinion that may change the processes organizations employ to create, maintain, search, produce and proffer electronic documents. The trouble started after the initial claim was paid, when the boat was pulled out of the water and damage to the hull was discovered under the waterline. The dispute related to the parties' enforcement of their arbitration agreement relating to this later-discovered damage. Each of the parties attached to their pleadings emails exchanged in the course of negotiating the arbitration agreement. In a major departure from current common practice regarding electronic communications, the opinion states that—even though neither party directly challenged the admissibility of the other's email evidence—the court was not in a

position to consider the emails, because no basis had been provided by the parties for admissibility or authentication.

How A Proponent Of Electronic Evidence May Lay Sufficient Foundation For Its Admission



Judge Grimm provides not only a review of the requirements for admitting electronic evidence under the Federal Rules of Evidence, but a practical discussion of some of the technology and document management issues raised by those requirements, such as hash values and other indicia of authenticity, metadata and collection techniques.¹ He notes cor-

rectly that while there has been extensive discussion of the rules regarding discovery of electronically stored information (“ESI”), very little has been written about “what is required to insure that ESI obtained during discovery is admissible into evidence at trial, or whether it constitutes ‘such facts as would be admissible in evidence’ for use in summary judgment practice.” He does not ignore the complexity arising from the evidentiary “flavors,” including e-mail, website ESI, internet postings, digital photographs, and computer-generated documents and data files.² He notes that courts have recognized that authentication of ESI may require greater scrutiny than for the authentication of “hard copy” documents, but “they have been quick to reject calls to abandon the excising rules of evidence when doing so.”³

Judge Grimm discussed five evidence standards ESI evidence must satisfy: (1) is the ESI relevant (under Rule 401); (2) is it authentic (under Rule 901(a)); (3) is it hearsay (under Rule 801) and, if so, does it constitute an exception under Rules 803, 804 and 807, (4) does it comply as an original

or duplicate under the original writing rule or, if not, can it be admitted pursuant to the admissible secondary evidence rules 1001-1008 to prove the content of ESI and (5) is the probative value of the ESI substantially outweighed by the danger of unfair prejudice or another factor identified by Rule 403.⁴

1. Relevance

Judge Grimm notes that proving that ESI has some relevance (i.e., evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable) is not hard for counsel, but urges for ESI articulating all of what may be multiple grounds of relevance.⁵

2. Authentication

More complex is the requirement that ESI be shown to be authentic (that the matter in question is what the proponent claims under rules 901 and 902). Authentication of ESI may require greater consideration than required for paper documents, and courts will demand that proponents of ESI evidence pay more attention to the foundation requirements than has been customary for introducing paper evidence. Yet Judge Grimm notes only a prima facie showing is required, but counsel often fail to meet this minimal showing.⁶

While 901(a) addresses the requirement to authenticate, Rule 901(b) provides ten non-exclusive examples of how authentication of electronically generated or stored evidence may be accomplished.⁷ The important thing is to plan in advance how the electronic evidence will be authenticated because Courts have accepted a number of the methods discussed in Rule 901(b) as well as some methods not included in the Rules.

Judge Grimm focuses on these 901(b) examples:

- ♦ 901(b)(1) Testimony of witness with knowledge;⁸
- ♦ 901(b)(3) authentication by “[c]omparison by the trier of fact or by expert witnesses

with specimens which have been authenticated;”⁹

- ♦ The frequently-used Rule 901(b)(4), which permits authentication by circumstantial evidence;¹⁰
- ♦ Metadata may also be used to authenticate electronic evidence under Rule 901(b)(4).¹¹
- ♦ Proof of custody of public records or reports under Rule 901(b)(7);¹² and
- ♦ “Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result” under Rule 901(b)(9).¹³

Rule 902 may also be used for authentication. ESI may be authenticated without extrinsic evidence by the 12 methods set forth in Rule 902. Rule 902 has the advantage of not requiring the sponsoring testimony of any witness to authenticate the exhibit since its admissibility is determined simply by examining the evidence itself, along with any accompanying written declaration or certificate required by Rule 902. “Although all of the examples contained in Rule 902 could be applicable to computerized records, three in particular have been recognized by the courts to authenticate electronic evidence: 902(5) (official publications); 902(7) (trade inscriptions); and 902(11) (certified domestic records of regularly conducted activity).” See, as an example of 902(5), *Equal Employment Opportunity Commission v. E.I. DuPont de Nemours and Co.*, 2004 WL 23457556 (E.D. La. Oct 18, 2004) (printouts of postings on the website of the United States Census Bureau were admitted into evidence as self-authenticating under Rule 902(5)).¹⁴

Courts have also embraced non-traditional methods of authentication. In

Telenizja Polska USA, 2004 WL 2367740, the Court determined that exhibits depicting the content of the defendant’s website at various dates several years in the past were admissible, based on an “affidavit from a representative of the Internet Archive Company, which retrieved copies of the defendant’s website as it appeared at relevant dates to the litigation through use of its ‘wayback machine.’”¹⁵

“Little could the owner or insurer of the pleasure boat Chessie have known that the lightning that struck Chessie would ultimately ignite a 101-page opinion that may change the processes organizations employ to create, maintain, search, produce and proffer electronic documents. ”

Judge Grimm notes that there are many ways in which email evidence may be authenticated, with the most frequent ways being “901(b)(1) (person with personal knowledge), 901(b)(3) (expert testimony or comparison with authenticated exemplar), 901(b)(4) (distinctive characteristics, including circumstantial evidence), 902(7) (trade inscriptions), and 902(11) (certified copies of business

record).”¹⁶ The other common forms of ESI discussed by Judge Grimm are Internet Website Postings,¹⁷ Text Messages and Chat Room Content,¹⁸ Computer Stored Records and Data,¹⁹ Computer Animation and Computer Simulations²⁰ and Digital Photographs.²¹ He recognizes that there is no single approach to authentication that will work for all such diverse media types.

Judge Grimm contrasts the lenient approach of admissibility of computer records by the Tenth Circuit in *United States v. Meienberg*, 263 F.3d 1177, 1180-81 (10th Circuit 2001), where evidence or printouts of computerized records of the Colorado Bureau of Investigation were admitted, with *In re Vinbee*, 336 B.R. 437-445 (B.A.P. 9th 2005), which excluded business records of the credit card issuer of a Chapter 7 debtor, for failing to authenticate them.²² Judge Grimm recognizes that more courts have tended to be lenient, rather than requiring

the demanding approach, but that commentators and courts increasingly recognize the special characteristics of electronically stored records and the need to consider the accuracy and reliability of computerized evidence in ruling on its admissibility.²³

3. Hearsay

The third requirement for admissibility of ESI emphasized by Judge Grimm is hearsay. As Judge Grimm noted, “[h]earsay issues are pervasive when electronically stored and generated evidence is introduced.” At issue are Rules 801-807 and Judge Grimm cites five separate questions that must be answered: (1) Does the evidence constitute a statement (Rule 801(a))?, (2) was the statement made by declarant (Rule 801(b))?, (3) is the statement being offered to prove the truth of its contents (Rule 801(c))?, (4) is the statement excluded from the definition of hearsay (Rule 801(1))?, and (5) if the statement is hearsay, is it covered by one of the exceptions identified at Rules 803, 804 or 807? Hearsay and its applicability to ESI are discussed in depth by Judge Grimm, who raises important issues when planning for admissibility of electronic information.²⁴

4. Original Writing Rule

The next evidentiary issue Judge Grimm evaluates for the admissibility of electronic evidence concerns application of the Original Writing Rule under Rules 1001-1008. The rules require an “original to prove the contents of a writing, recording or photograph unless secondary evidence is deemed acceptable.”²⁵

An issue that Judge Grimm explains will arise in certain cases is whether the Original Writing Rule applies at all. Judge Grimm cites an example of when the Original Writing Rule did apply to electronic evidence involving a police officer cutting and pasting the text of the text messages from an internet chat room into a word processing program. The printouts, which were then introduced into evidence, were prepared from the program. The Court found that the State was

proving the content of a writing, but that the printout was an original, and could be found to be the “Best Evidence” of the conversations at issue.²⁶

Of Judge Grimm’s discussion of Rules 1001-1008, relating to the Original Writing Rule and secondary evidence, certain points deserve special mention. Rule 1004, involving the use of secondary evidence, identifies four circumstances in which secondary evidence may be introduced instead of an original. The first circumstance is, “Originals lost or destroyed. All originals are lost or have been destroyed, unless the proponent lost or destroyed them in bad faith.” Judge Grimm notes that this first circumstance may be particularly suited for electronic evidence, and citing FRCP 37(f)’s new, limited “safe harbor,” states that “the new rule evidences the widespread recognition that electronically stored information is not infrequently lost or destroyed.”²⁷

Another noteworthy reference is Rule 1006, which recognizes another source of secondary evidence to prove the contents of voluminous writings, recordings or photographs.²⁸ Judge Grimm stated that “[b]ecause the production of electronically stored information in civil cases frequently is voluminous, the use of summaries under Rule 1006 is a particularly useful evidentiary tool, and courts can be expected to allow the use of summaries provided the procedural requirements of the rule are met.”²⁹

5. Balancing Probative Value Against Unfair Prejudice

The final step to consider with regard to electronically prepared or stored evidence raised by Judge Grimm is the need to balance its probative value against the potential for unfair prejudice or other harm

under Rule 403. Judge Grimm suggests four circumstances where courts, under Rule 403, are particularly likely to consider whether the admission of electronic evidence would be unduly prejudicial: (1) When the evidence would contain offensive or highly derogatory language that may provoke an emotional response; (2) when analyzing computer animations, to determine if there is a substantial risk that the jury may mistake them for the actual



events in the litigation; (3) when considering the admissibility of summaries of voluminous electronic writings, recordings or photographs under Rule 1006; and (4) in cir-

cumstances when the court is concerned as to the reliability or accuracy of the information that is contained within the electronic evidence.³⁰

Processes That Mitigate Risks Of Failure Along The ESI Value Chain

Judge Grimm’s mini-treatise is a must read for those involved in designing and implementing effective e-contracting processes and systems, and processes for the creation and maintenance of ESI more generally. Vendors developing document management and content management systems need to incorporate a strategy for admissibility of ESI into the entire ESI value chain, from creation to maintenance, custody, security and access rules, to search, preservation, production and admission as evidence, to destruction. All along this chain the ESI faces risks of failing, for example failing to be admissible, to be enforceable or to be persuasive. Judge Grimm raises many such risks of failure, and also implies—sometimes much less directly—processes for mitigating and managing those risks.

In the past five or more years, such processes have been under examination and development in connection with electronic signature law. The electronic signature laws in the U.S., both the state enactments of the Uniform Electronic Transactions Act, or UETA, that is in effect in forty-six states, and the federal ESIGN Act that applies in the other four and in certain federal matters, clearly provide that signatures may not be denied solely because they are electronic, and contracts formed exclusively through electronic means may not be denied solely because they are in electronic form. Neither ESIGN nor UETA give higher status to electronic signatures or e-contracts than to signatures or contracts signed using wet ink on paper. All the other rules and legal principles applicable to signature and contracts, including rules of evidence, apply equally to e-records and e-contracts.

If the ultimate goal of an e-signature is to enforce the terms of the record on which it appears against its signer, the person seeking to enforce that record must meet the admissibility threshold described by Judge Grimm. The proponent needs to be able to persuade a jury of the terms of the e-contract and that the other person signed it. To get the document before the jury, the e-contract with the e-signature needs to be admissible as evidence. To establish the terms associated with an e-signature it is necessary to understand both the rules for authenticating the e-document and the essential elements of an effective e-signature and e-contracting process. Litigators and designers of document management systems need to be aware of these and other ways in which the authentication of ESI can be challenged under ESIGN and UETA as well as under the Federal Rules of Evidence.

For example, to introduce a hard copy of the terms and conditions of a contract formed using e-signatures at a company's website may require a credible witness at the company to testify or swear to the e-contracting process as a way to authenticate the hard copy of such record bearing the party's signatures. In testifying about the e-con-

tracting process and why the witness is confident that the hard copy accurately reflects the e-contract as it was in fact formed, the witness may be challenged on the various steps taken by the company to verify the identity of the person signing the e-contract, to secure the e-record after the e-contract was signed, to securely archive and retrieve the electronic record and a host of other aspects of the e-contracting and ESI management processes.

An effective e-contracting process addressing such topics can withstand such challenges at the admissibility phase as well as enhance the overall credibility of the hard copy as a true and accurate record of the e-record. Creating and securely archiving and retrieving an audit trail of the entire ESI management process, from the steps to verify the identity of the persons signing the record all the way through to sealing electronically the document and then securely archiving and retrieving the e-contract are examples of essential elements of an effective e-contracting process. These same steps enhance the overall persuasiveness of the hard copy of the e-contract as well.³¹

This *Client Alert* can only highlight some of the ESI and evidentiary issues discussed so well by Judge Grimm, and can only offer a brief glimpse of the implications of those issues for ESI management processes. More on this topic will surely follow.

End Notes

1. All references to rules herein refer to the Federal Rules of Evidence. The page numbers in parentheses cite to Judge Grimm's Memorandum Opinion as originally published by the Court.
2. P. 8.
3. P. 18. Judge Grimm cites, for example, *In Re F.P., A Minor*, 878 A.2d 91, 95 (Pa. Super. Ct. 2005) ("Essentially, appellant would have us create a whole new body of law just to deal with e-mails or instant messages . . . we believe that e-mail messages and similar forms of electronic communications can be properly authenticated within the existing framework of [the state rules of evidence].") (pp. 18-19). See

also the cases cited by Judge Grimm including *In Re Vee Vinbee*, 336 B.R. 437 444 (B.A.P. 9th 2005) and *United States v. Safavian*, 435 F.Supp. 2d 36, 41-42 (D.D.C. 2006).

4. P. 9.

5. Pp. 15-16.

6. P. 17. Judge Grimm quotes from *Weinstein's Federal Evidence*, [Jack B. Weinstein & Margaret A. Berger, *Weinstein's Federal Evidence* (Joseph M. McLaughlin ed., Matthew Bender 2d ed. 1997) (hereinafter, "Weinstein")] at Section 900.06[3]. that "In general, electronic documents or records that are merely stored in a computer raise no computer-specific authentication issues. If a computer processes data rather than merely storing it, authentication issues may arise...The authentication requirements of Rule 901 are designed to set up a threshold preliminary standard to test the reliability of evidence. . . Factors that should be considered in evaluating the reliability of computer-based evidence include the error rate in data inputting, and the security of the systems. The degree of foundation required to authenticate computer-based evidence depends on the quality and completeness of the data input, the complexity of the computer processing, the routineness of the computer operation, and the ability to test and verify results of the computer processing." (pp.18-19)

7. P. 20

8. P. 22

9. P. 23. In *Safavian*, 435 F.Supp. at 40, the Court accepted 901(b)(3) as appropriate for authenticating email.

10. P. 24. See *United States v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir. 2000). Judge Grimm noted that one method under Rule 901(b)(4) is the use of "hash marks" when making documents, and that "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). Also they can be used during discovery or electronic records to create a form of electronic 'Bates stamp' that will help establish the document as electronic." *Citing Federal Judicial Center, Managing Discovery of Electronic Information, A Pocket Guide for Judges, Federal Judicial Center, 2007 at 24, United States District Court for the District of Maryland, Suggested Protocol for Discovery of Electronically Stored Information 20.*

11. Judge Grimm notes that under recently revised Federal Rule of Civil Procedure 34, a party may discover electronically stored information in its "native format" which includes

Office Locations

ATLANTA

CHICAGO

LONDON

LOS ANGELES

NEW YORK

SACRAMENTO

WASHINGTON

www.lordbissell.com

the metadata for the electronic document. As Judge Grimm explained “[b]ecause metadata shows the date, time and identity of the creator of an electronic record, as well as all changes made to it, metadata is a distinctive characteristic of all electronic evidence that can be used to authenticate it under Rule 901(b)(4).” (p. 26- 27)

12. Judge Grimm cited the FRE 901(b) Advisory Committee Notes, which states that public records are regularly authenticated by proof of custody, without more, and that 901(b)(7) “extends the principle to include data stored in computers and similar methods, of which increasing use in the public records area may be expected.” (p.28)

13. Pp. 29-30. This is “particularly useful in authenticating electronic evidence stored in or generated by computers.”

14. Pp. 30-34.

15. “The ‘wayback machine’ refers to the process used by the Internet Archive Company, www.archive.org, to allow website visitors to search for archived web pages of organizations *St. Lukes*, 2006, WL 1320242 at *1. (p.37)

16. P. 40. In addition to Weinstein, at § 900.07[3][c], Judge Grimm also cites, as a useful reference, *Edward J. Imwinkelried, Evidentiary Foundations* § 403[4][b] (*LexisNexis 6th ed.* 2005).

17. P. 41.

18. P. 43.

19. P. 44.

20. P. 49.

21. P. 52.

22. P. 47. That court adopted, with some modification, an 11-step foundation proposed by Professor Imwinkelried (in § 403[2], *Imwinkelried, Evidentiary Foundations*).

23. Citing the Manual for Complex Litigation at §11.446.

24. Pp. 56-83.

25. P. 83. Judge Grimm states that traditionally this has been referred to as the “Best Evidence Rule;” he prefers the “Original Writing Rule,” since “secondary evidence” in certain instances may be used. Citing *Weinstein*, at § 900.07[1][d][iv], Judge Grimm states that the Original Writing Rule has particular applica-

bility “to electronically prepared or stored writings, recordings or photographs.” (p. 85)

26. *Laughner v. State*, 769 N.E.2d 1147 (Ind. Ct. App. 2002), *abrogated on other grounds by Farjardo v. State*, 859 N.E.2d 1201 (Ind. 2007). (p. 89)

27. “Given the myriad ways that electronic records may be deleted, lost as a result of system malfunctions, purged as a result of routine electronic records management software (such as the automatic deletion of e-mail after a set time period) or otherwise unavailable means that the contents of electronic writings may have to be proved by secondary evidence” (p. 91)

28. P. 91.

29. P. 94. *See, e.g., Wapnick v. Comm’r of Internal Revenue, T.C. Memo*, 2002-45 (T.C.2002).

30. Pp. 98-100.

31. In some cases, a person may seek to introduce the ESI itself, and not a hard copy of the record, in which case the person will still need to authenticate the electronic record, using other authentication steps described by Judge Grimm. For more information on implementing e-contract and e-discovery readiness processes, see:

http://www.lordbissell.com/newsstand/eSignatures_BTG.pdf
and

http://www.lordbissell.com/Newsstand/InformationMgmt_BTG.pdf

ABOUT THE AUTHORS

Lord, Bissell & Brook LLP has a leading practice in advising corporations about electronic discovery and e-records management. Jon Neiditz leads Lord, Bissell & Brook LLP’s Information Management Practice, and has led over 60 engagements focused on e-discovery readiness and related information management issues. Jay Safer has experience in complex litigation and arbitrations and chairs the New York City Bar Association’s Council on Judicial Administration. Pat Hatfield chairs the Business Technology Group and assists clients develop and manage solution sets in the area of e-commerce, including e-signatures, e-record retention, privacy, security, and technology-related dispute resolution.