Lorraine v. Markel: Electronic Evidence 101

LexisNexis®

Common Types of Electronically Stored Information

Email: Rules 901(b)(1) (person with personal knowledge); 901(b)(3) (expert testimony or comparison with authenticated example); 901(b)(4) (distinctive characteristics, including circumstantial evidence); 902(7) (self-authentication by inscriptions); and 902(11): authentication of regularly conducted business).

Internet Web Site Postings: 901(b)(1) (witness with personal knowledge); 902(b)(3) (expert testimony); 901 (b)(4)(distinctive characteristics; 901 (b)(7)(public records); 902 (b)(9) (system or process capable of producing a reliable result); and 902(5)(official publications)

Text Messages and Chat Room Content: 901(b)(1)(witness with personal knowledge) and 901 (b)(4)(circumstantial evidence of distinctive characteristics).

Computer Stored Records and Data: 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).

Computer Animation and Computer Simulations: 901(b)(1) (witness with personal knowledge); 901(b)(3) (expert witness). May also require the use of an expert witness under FRE 702 and 703.

Digital Photographs: 901(b)(1) (witness with personal knowledge).

Lorraine v. Markel: Electronic Evidence 101

While most of us have been focusing on the *discovery* of electronically stored information, the ultimate use of that evidence at trial and its admissibility have often been overlooked. Not so by Judge Paul W. Grimm, Chief Magistrate Judge from the District of Maryland who has written a 101-page opinion on precisely how to get electronically stored information into evidence. An essential primer on evidence admission, *Lorraine v. Markel American Insurance Co.*, 2007 U.S. Dist. LEXIS 33020 (D. Md. May 4, 2007) nicely lays out some of the problems with the admissibility of electronically stored information and provides key guidance on some of the strategic ways to proffer this evidence in federal court.

The *Lorraine* Case: Background

Lorraine involved an insurance dispute over the recovery of insurance proceeds after the Plaintiff's boat was struck by lightening. Defendant insurance company paid out under the policy. Plaintiff later discovered that there had been damage to the ship's hull and claimed that he was entitled to an additional $36,000 to fix that damage. Defendant disagreed. Plaintiff filed a claim against his insurance company and the matter went to arbitration. At arbitration, the arbitrator held that some of the damage to the boat's hull had been caused by the lightening but limited the damages to $14,000. The issue in the district court was whether the arbitrator exceeded his authority by reducing the damages to $14,000. Plaintiff claimed the arbitrator was only authorized to determine whether the ship's hull was damaged as a result of the lightening; Defendant claimed the arbitrator had the authority to reduce the award.

Both parties filed motions for summary judgment and both parties attached as exhibits emails that discussed the policy at issue. Neither party, however, supplied any authentication for the emails such that they would be admissible to support a motion for summary judgment. Judge Grimm thus took the opportunity of this case to discuss how electronically stored information can be proffered such that it is admissible into evidence.

How to get Electronically Stored Information into Evidence

Judge Grimm starts out by recognizing that to get electronically stored information into evidence, a series of evidentiary "hurdles" must be overcome, specifically, the following Federal Rules of Evidence (FRE) rules must be considered: Rules 104, 401, 901 and 902, 801, 1001-1008 and rule 403. He then discusses each rule at length:

Rule 104: Preliminary Questions

Judge Grimm first considered the applicability of Rule 104 to the admissibility issue. Rule 104 addresses the relationship between the judge and the jury with regard to preliminary fact finding associated with the admissibility of evidence. In short, under Rule 104, the court, must determine whether there is a foundation for authenticity. In so doing, the court may consider evidence that might not otherwise be admissible. But because authentication is ultimately a question of "conditional relevancy," the jury is responsible for determining whether it is authentic. The jury can only consider that which is otherwise admissible in making its determination. In the context of electronically stored information, Judge Grimm offered this example:

> If an e-mail is offered into evidence, the determination of whether it is authentic would be for the jury to decide under Rule 104(b), and the facts that they consider in making this determination must be admissible into evidence. In contrast, if the ruling on whether the e-mail is an admission by a party opponent or business record turns on contested facts, the admissibility of those facts will be determined by the judge under 104(a) and the Federal Rules of Evidence, except for privilege, are inapplicable. *Lorraine*, at *23-24.

Rule 401: Relevance

The first requirement for admissibility is that the evidence must be relevant under Federal Rule of Evidence 401, which is "having any tendency to make the existence of any fact" "more or less probable." *Id.* at *25 (citing FRE 401). Judge Grimm points out that "there is a distinction between the admissibility of evidence and the weight to which it is entitled in the eyes of the fact finder" and that to be relevant, evidence does not have to carry any particular weight: "it is sufficient if it has 'any tendency' to prove or disprove a consequential fact in the litigation." *Id.* at *27.

Judge Grimm then determined that the emails in the case that had been attached to the motions for summary judgment were, in fact, relevant, meeting the requirements of Rule 401.

Rule 901: Authenticity

If evidence is not relevant, the inquiry ends, as "evidence that is not relevant is never admissible." If it is relevant, all of the other rules are designed to determine whether relevant evidence "should nonetheless be excluded." *Id.* at 28.

Rule 901 defines authentic evidence as that which is supported by "a finding that the matter in question is what its proponent claims." *Id.* at *30 (citing FRE 901). With respect to electronically stored information, Judge Grimm states that "counsel often fail" to meet the minimum required for authenticity, which is merely a prima facie showing of authenticity.

Although Rule 901 addresses the requirement to authenticate electronically stored evidence, Judge Grimm points out that it is "silent" on how to do so." *Id* at *37. Judge Grimm then points out several examples in 901(b) that help illustrate how electronically stored information may be authenticated through the use of extrinsic evidence:

1) **Testimony of witness with knowledge: Rule 901(b)(1).** The authenticating witness must "provide factual specificity about the process by which the electronically stored information is created, acquired, maintained, and preserved without alteration or change or the process by which it is produced if the result of a system or process that does so."

2) **Comparison by the trier of fact or by expert witnesses with specimen which have been authenticated. Rule 901(b)(3).** In the context of electronically stored information, this can be fulfilled by comparing emails previously authenticated with the evidence in question.

3) **Circumstantial evidence of the evidence itself. Rule 901(b)(4).** This rule is the most frequently used to authenticate email, as the content of what the email says can often authenticate it. See *United States v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir. 2000). Another way to satisfy this rule is through hash marks, which is a unique identifier attached to electronic information, and metadata which also provides distinguishing information about the evidence.

4) **Public Records. Rule 901(b)(7).** This rule applies when the proponent of the evidence can show that the office from which the electronic records were taken is the legal custodian of the records. There is no need to show that the computer system producing the records was reliable or the records accurate. Any question as to accuracy goes to the weight of the of the evidence rather than admissibility. *Lorraine* at *53.

5) **Evidence produced as a result of an accurate process or system. Rule 901(b)(9).** In the e-discovery context, this rule is satisfied by "evidence describing the process or system used to achieve a result and demonstration that that result is accurate." *Id.* at *55.

Rule 902: Self-Authentication

Rule 902 illustrates how authentication can be achieved without extrinsic evidence, i.e., through "self-authentication." Although the rule lists twelve examples of self-authentication, Judge Grimm points out that three of the examples have been used in the courts to authenticate electronically stored information:

1) **Official publications. Rule 902(5).** In order to be admissible, a proponent may also need to establish that the official publication qualifies as a public hearsay record under Rule 803(8). An example of self-authenticated evidence under this rule would be a posting on the Web site of the *United States Census Bureau. Equal Opportunity Commission v. E.I. DuPont De Nemours and Co.*, 2004 U.S. Dist. LEXIS 20748 (E.D. La. 20748).

2) **Self-authentication by inscriptions, signs, tags or labels. Rule 902(7).** Here, business e-mails that contain information showing the origin of the transmission and identifying the employer company may be sufficient to authenticate and email. *Lorraine* at *65, citing Weinstein at § 900.07[3][c].

3) **Authentication of Regularly Conducted Business. Rule 902(11).** This rule requires a party to fulfill all of the requirements of Rule 803(6), which is the business record exception to the hearsay rule, thus killing two birds with one stone.

Judge Grimm also notes that while these examples are not exclusive, courts have been creative with ways to allow authentication. For example, one court has held that any documents produced in discovery are presumed to be authentic, that is, that a party cannot produce information in discovery and then claim that the opposing party must prove authenticity. *Id.* at *68, citing *Indianapolis Minority Contractors*, Ass'n v. Wiley, 1998 U.S. Dist. LEXIS 23349 (D.Ind. May 13, 1998).

Authentication can also be established by judicial notice; by taking advantage of Federal Rule of Civil Procedure 36 (requesting opposing party admit to genuineness of document); via stipulation at a pretrial conference pursuant to Federal Rule of Civil Procedure (FRCP) 16 (c)(3); and pursuant to FRCP 26, which gives a party 14 days to file objections to opposing party's Rule 26 disclosures. Failure to do so waives all objections except under rules 402 and 403.

Rule 801: Hearsay

Although the parties in *Lorraine* had not properly authenticated the emails attached to their motions, Judge Grimm nonetheless proceeded with the analysis required for the admission of electronically stored information into evidence. That is, once evidence is relevant and authentic, it must also overcome any hearsay objections.

In the context of electronic evidence, the issue at the heart of Rule 801 is whether electronic writings constitute statements by a declarant within the meaning of Rule 801(a). A computer generated printout, for example, does not involve a person so it cannot be hearsay. Likewise, the header on a fax that displays the time it was sent is not hearsay. *Lorraine* at *113, citing *United States v. Khorozian*, 2003 U.S. App. LEXIS 12703 (3rd. Cir. 2003). Hearsay is also defined as a statement being made "to prove the truth of what is asserted." For example, an email offered to prove that a relationship existed between the two parties to the communication is not hearsay. *See, e.g. United States v. Siddiqui*, 2000 U.S. App. LEXIS 31882 (11th Cir. 2000). Similarly, as the emails at issue in *Lorraine*, emails between parties to a contract that define the terms of a contract, or prove its content are not hearsay. The hearsay rules also provide several exceptions to the definition of hearsay in Rule 801(d)(1) and 801(d)(2). 801(d)(2) is most often used as an exclusion to the hearsay rule in the context of email because is excludes "admission by a party opponent."

Rules 803, 804 and 807 provide several exceptions to the hearsay rule. All in all there are 29 exceptions to the hearsay rules. Judge Grimm takes on the "daunting task" of applying these to electronically stored information by grouping them into three categories. He then analyzes the exceptions that are most applicable to electronically stored information, including:

- Rule 803(1): Present Sense Impression
- Rule 803(2): Excited Utterance
- Rule 803(3): Then Existing State of Mind or Condition
- Rule 803(6): Business Records
- Rule 803(8): Public Records
- Rule 803(17): Market Reports, Commercial Publications

Finally, Judge Grimm noted that with hearsay, unless it is objected to, it will generally be admitted, "which underscores the need to pay attention to exhibits offered by an opponent, as much as to those records that you need to introduce. A failure to raise a hearsay objection means that the evidence may be considered for whatever probative value the finder of fact chooses to give it." *Lorraine* at *154.

Rules 1001 – 1008: The Original Writing Rule

The next hurdle that evidence must overcome is the Original Writing Rule, often referred to as the "Best Evidence Rule." Under Rule 1003, duplicates can be admitted into evidence in lieu of the original unless there are issues of authenticity of the original. This is of particular concern with electronically stored evidence, as it is often difficult to share or mark as an exhibit if it is displayed on a screen. Commentators have noted that "so long as it accurately reflects the data," print out of these kinds will be admissible. *Id.* at *163, citing *Weinstein* § 900.07[1][d][iv]. *See also, Laughner v. State*, 769 N.E.2d 1147 (Ind. Ct. App. 2002), *abrogated on other grounds by Farjardo v. State*, 859 N.E. 2d. 1147 (Ind. 2007) (printout of emails shown to reflect the data accurately is an original). Failure to properly raise an objection to best evidence at trial will result in waiver of the error on appeal. *Lorraine* at *168.

Rule 403: Balance of Probative Value with Unfair Prejudice

The final evidentiary rule that must be observed is Rule 403, which balances the need to balance the probative value of the evidence against the potential for unfair prejudice. Electronically stored information has been found to be unduly prejudicial when it contains offensive or highly derogatory language; when there is substantial danger that a jury might mistake computer animation for actual events; when considering summary evidence; and when the court is concerned as to the reliability of the accuracy of the information.

Conclusion: E-Discovery Best Practices Equal E-Evidence Best Practices

With all of the focus on e-discovery over the past few years, it was only a matter of time before the courts started to focus on e-evidence. From the dearth of cases cited by *Lorraine*, it is clear that this is an area that is only now developing. Judge Grimm makes it clear, however, that failure to pay attention to the issues raised by admissibility may damage a case just as severely as any e-discovery sanction. The good news is that many of the same best practices applied to e-discovery, also apply to admissibility of evidence.

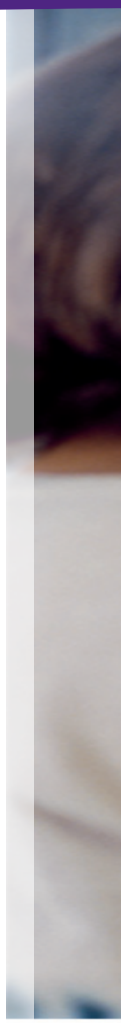
For example, in his discussion of Rule 901, Judge Grimm points out that one of the problems with the authenticity of electronically stored information is that "computerized data ... raise unique issues concerning accuracy and authenticity ... The integrity of data may be compromised in the course of discovery by improper search and retrieval techniques, data conversion, or mishandling." *Id.* (citing *In re Vee Vinhee*, 2005 Bankr. LEXIS 2602 (9th Cir. Bankr. Panel Dec. 16, 2005) and the Manual for Complex Litigation at § 11.447). This is a key point for litigants who self-collect electronically stored data or rely on outside counsel to do so. Special care must be taken to ensure proper collection methods. If a company or law firm does not have the requisite expertise to properly collect data, they would be wise to seek help from an expert. For although 901 is silent on how to properly authenticate, a professional e-discovery service provider will follow proper chain of custody protocols that minimize any issues that could compromise the evidence.

Similarly, Rule 901(b)(1) allows for authentication through the testimony of witness with knowledge. Much has been written about the need for companies to prepare a 30(b)(6) witness to testify about information technology systems in corporations involved in litigation for the discovery process; here that same witness can also help authenticate data at trial.

Probably the most effective strategy a company can employ to help ensure that evidence is admitted at trial is to have a comprehensive records retention policy. A good records retention policy can help with both self-authentication under Rule 902(11) (authentication of regularly conducted business) and an exception to the

hearsay rules under 803(6)(exception for business records). With e-discovery, having a working, wide-ranging records retention policy can assist parties with their obligations under the new Federal Rules of Civil Procedure. But it can also have the added benefit of providing a foundation for admissibility at trial. *See, e.g., State of New York v. Microsoft*, 2002 U.S. Dist. LEXIS 7683 (D.D.C. Apr. 12, 2002) (cited in *Lorraine* for the proposition that an email did not qualify as a business record because there had been no showing that the practice of the employee to send an email following the receipt of a phone call was the regular practice of the employer to require that the employee make and maintain such emails). The opposite should then also be true: emails from a company that does have a records retention policy should be excepted from hearsay under Rule 803(6) and properly authenticated under Rule 902(11).

We often forget that preparing for e-discovery is just the beginning of the process of preparing for trial. *Lorraine* reminds us that parties who often find themselves in litigation would be wise to think beyond the discovery of electronically stored information to the ultimate use of that information. Even more importantly, companies should think of the litigation process as merely one piece in the entire lifecycle of their records: from creation, to storage, to preservation, to collection, to use a trial, all the way through until the information is no longer needed, preserving the integrity and ultimate usability of that information from beginning to end.



The Discovery Experts: Industry Relations

Discovery Services from LexisNexis® has the right consulting and technology choice for every discovery need. Top law firms, corporations and government agencies rely on the LexisNexis® products and services, Applied Discovery®, Concordance®, Hosted FYI™, and LAW PreDiscovery™ to meet their discovery obligations on time, accurately and cost-effectively. Services include records-management consulting, data collection, forensics, media restoration, data filtering, data processing, review and document production in the format that each matter requires. The Industry Relations team works to educate the legal community on the continually evolving case law and technology of electronic discovery.

For more information or to contact the experts, please visit **lexisnexis.com/discovery**.

LexisNexis®