Illinois Association of Defense Trial Counsel
Springfield, Illinois | www.iadtc.org | 800-232-0169
IDC Quarterly | Volume 18, Number 1 (18.1.35)

E-Discovery

By: Peter R. Jennetten
Quinn, Johnston, Henderson & Pretorius, Peoria

From E-Discovery to E-Evidence: *Lorraine v. Markel American Ins. Co.*

It is one thing to obtain a mountain of electronically stored information (ESI) from an opponent in discovery. It is another to get it admitted into evidence. Chief United States Magistrate Judge Paul W. Grimm of the District of Maryland provided an outline of the issues in *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007). The lengthy opinion is a compendium of issues and case law addressing the admissibility of ESI.

Lorraine involved petitions to enforce an arbitration award arising out of an insurance coverage dispute over lightning damage to a yacht. The parties filed cross-motions for summary judgment supported, in part, by e-mails pertaining to the negotiation of the arbitration agreement. The court began by noting that there were five areas of evidence law to consider:

> 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 Rule 401 * * * (2) * * * is it authentic as required by Rule 901(a) * * * (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 * * * (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 * * * 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. *Lorriane*, 241 F.R.D. at 538.

Relevance and the Rule 403 balancing do not differ materially from other forms of evidence, but ESI raises unique issues with respect to the other factors.

Authentication

The *Lorraine* court noted that a party "need only make a prima facie showing that [the exhibit] is what he or she claims it to be." *Id*. at 542. This concept is governed by Rules 901-902. The most common method of authenticating ESI is by testimony from a witness with knowledge of the exhibit. Fed. R. Civ. P. 901(b)(1); *Lorraine*, 241 F.R.D. at 545. This does not need to be the person who generated the ESI. Other methods of authentication may be particularly useful for ESI.

Some exhibits, such as e-mail, can be authenticated by comparing the questioned document to one known to be authentic. The comparison can be made by expert testimony or by the trier of fact. Using this method, ESI is authenticated by its "distinctive characteristics, taken in conjunction with circumstances." Fed. R. Civ. P. 901(b)(3). Judge Grimm noted that this has been applied in a variety of cases to authenticate e-mail, website content and text messages. *Lorraine*, 241 F.R.D. at 546 (citations omitted). Applications include "authenticating an exhibit by showing that it came from a particular person by virtue of its disclosing knowledge of facts known peculiarly to him, or authenticating by content and circumstances indicating it was

in reply to a duly authenticated document." *Id*. (punctuation omitted). This also could include authentication by the use of digital "hash marks" or by examination of the exhibit's metadata. *Id.* at 546-47.

Public records or reports comprising ESI can be easily authenticated pursuant to Fed. R. Civ. P. 901(b)(7). This could apply to a variety of records including "tax returns, weather bureau records, military records, social security records, INS records, VA records, official records from federal, state and local agencies, judicial records, correctional records, law enforcement records * * *." *Lorraine*, 241 F.R.D. at 548. The "proponent of the evidence need only show that the office from which the records were taken is the legal custodian of the records." *Id.* (*citing* Weinstein's Federal Evidence §901.10(2)). ESI generated by computers can also be authenticated under Rule 901(9), which requires evidence "describing a process or system used to produce a result and showing that" it does so accurately. *Lorraine*, 241 F.R.D. at 549.

Some ESI will be self-authenticating pursuant to Fed. R. Evid. 902. There are 12 categories within this rule, including "official publications * * * purporting to be issued by public authority." Fed. R. Evid. 902(5). For example, printouts from the Census Bureau website have been authenticated this way. *Lorraine*, 241 F.R.D. at 551 (citing case). Before the exhibit is admitted, the proponent may need to show that it is also a "public record" to avoid application of the hearsay rule. *Id*.

Pursuant to Rule 902(7), some ESI may be self-authenticated by "[i]nscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin." Judge Grimm suggested that business e-mails showing the origin of the e-mail and identifying the sending company may be self-authenticating under this rule. *Id.* at 551-52, 554. Rule 902(11) is particularly helpful, as it parallels the business records exception to the hearsay rule (Fed. R. Evid. 803(6)). The downside is that notice must be given to all adverse parties in advance of submission. Fed. R. Evid. 803(6).

Judge Grimm also pointed out that the 10 methods of authentication provided in Rule 901(b) are illustrative, not exhaustive. The courts have found creative ways to authenticate ESI. For example, "documents provided to a party during discovery by an opposing party are presumed to be authentic, shifting the burden to the producing party to demonstrate that the evidence that they produced was not authentic." *Lorraine*, 241 F.R.D. at 552 (citations omitted). Keep in mind that this establishes only the authenticity of the ESI, not admissibility. In another case, the contents of a website at various points in time were authenticated by a third-party, who used its "wayback machine" to verify the contents and provided an affidavit authenticating the records. *Id.* at 553.

Hearsay

The rule against hearsay provides another potential bar to the admission of ESI. Computer-generated information is not subject to the hearsay rule. The federal hearsay rules apply only to "statements," which are defined as "(1) an oral or written assertion or (2) nonverbal conduct *of a person* * * *." Fed. R. Evid. 801(a), (c) (emphasis added). Because computer-generated information is not an assertion or conduct "of a person," it cannot be subject to the hearsay rule. *Lorraine*, 241 F.R.D. at 564-65. An example of this is the report generated by the fax machine when a fax is sent, indicating the sender, time sent, and number of pages. As long as the validity of the process is proven (e.g. proof that the clock was set properly and the fax machine was operating correctly), the evidence is authenticated under Rule 901(9) and is not subject to a hearsay objection. The Illinois Supreme Court similarly found that telephone traps or tracings recorded by computer were not hearsay. *People v. Holowko*, 109 Ill. 2d 187, 486 N.E.2d 877 (1985).

Electronic records such as e-mail, chat, and word processing documents may contain hearsay. The application of exceptions to the hearsay rule is generally straightforward (or as straightforward as for any other evidence). One fertile area of discussion has been whether e-mails constitute "business records" to satisfy that exception to the hearsay rule. Fed. R. Civ. P. 803(6). Courts have issued varying opinions in that regard. *See, Lorraine* 241 F.R.D. at 572-74.

Original Writing Rule

An original or duplicate of a writing is required to prove its content. Fed. R. Evid. 1001-1003. "Writings" includes any "electronic recording or other form of data compilation." Fed. R. Evid. 1001(1). "The 'original' of information stored in a computer is the readable display of the information on the computer screen, the hard drive or other source where it is stored, as well as any printout or output that may be read, so long as it accurately reflects the data." *Lorraine*, 241 F.R.D. at 577-78 (*citing* Rule 1001(3)). This defines the "original" of an electronic document very broadly and, by implication, expands the universe of "duplicates." For example, chat room text that was copied and pasted into a word processor was still considered an original record.

There are also several exceptions to the rule, which allow secondary evidence, including where the original is lost or destroyed. Fed. R. Civ. P. 1004. Given the ease with which ESI can be lost or destroyed, this is a particularly relevant exception. As Judge Grimm noted, these rules apply only where the proponent of the evidence seeks to prove the content of the record. *Id.* (*citing* Rule 1002). He found that the contents of the e-mails regarding the arbitration agreement were at issue in that case and chided counsel for failing to address the original writing rule in their proof or briefs.

Conclusion

Because counsel on both sides failed to authenticate the ESI or address other evidentiary issues, including hearsay, the original writing rule, and Rule 403, the judge dismissed both motions for summary judgment. This column provides only a brief overview of Judge Grimm's opinion, which was itself a concise overview of the issues raised in attempting to admit ESI in evidence. Undoubtedly, some courts will take a different view of some of the issues raised by Judge Grimm, but the opinion identifies many of the issues to be addressed, which is half the battle.

About the Author

Peter R. Jennetten is a partner with Quinn, Johnston, Henderson and Pretorius in Peoria. His practice includes civil rights, municipal liability, and general negligence. He can be reached via email at pjennetten@qjhp.com.