A Primer on the Admissibility of ESI in Bankruptcy Proceedings

Michael D. Fielding[1]
Husch Blackwell Sanders LLP[2]

Acknowledgement: *The author would like to thank Mary Mack, Esq., Brad Harris and Aaron Cronan of Fios, Inc.[3] for their helpful contributions regarding database ESI.[4]*

Part I: Generally applicable principles for admission of ESI

1) A must read decision is *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007). The *Markel* opinion is effectively a 51 page treatise which thoroughly explores the admissibility of ESI under the Federal Rules of Evidence.[5] This outline summarizes the key points of *Markel.* The author's oral presentation will address application of these rules of law in bankruptcy proceedings.

> ***"Given the pervasiveness today of electronically prepared and stored records, as opposed to the manually prepared records of the past, counsel must be prepared to recognize and appropriately deal with the evidentiary issues associated with the admissibility of electronically generated and stored evidence."***[6]

> ***"[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 or rejected from consideration during summary judgment because the proponent cannot lay a sufficient foundation to get it admitted."***[7]

---

[1] Michael D. Fielding is an associate attorney in the Insolvency and Commercial Bankruptcy practice group of Husch Blackwell Sanders LLP, 4801 Main Street, Suite 1000, Kansas City, MO 64112, (816) 983-8353 (direct), (816) 983-8080 (fax), michael.fielding@huschblackwell.com. He is licensed to practice law in both Kansas and Missouri. Mr. Fielding is certified by the American Board of Certification as a Business Bankruptcy Specialist.

[2] The views expressed in this outline are solely those of the author and do not necessarily represent the views or opinions of Husch Blackwell Sanders LLP.

[3] Fios is a Socha-Gelbmann "Top 5" electronic discovery services provider exclusively focused on delivering comprehensive services and expert guidance throughout all phases of the litigation process. The company may be contacted at Fios, Inc. c/o Aaron Cronan, Esq., 921 SW Washington St., Suite 850, Portland, Oregon 97205, (503) 808-1614, acronan@fiosinc.com

[4] *See* ¶ 12(e) below.

[5] The *Markel* opinion does not consider privilege issues due to inadvertent production.

[6] *Markel,* 241 F.R.D. at 537.

[7] *Id*. at 538

2) Overview: The admissibility of ESI for either trial or summary judgment will depend upon the following evidentiary points:[8]

a) Is the evidence relevant? FRE 401
b) Is the evidence authentic? FRE 901(a)
c) If offered for its substantive truth, is it hearsay and, if so, is there an exception for the hearsay? FRE 801, 802, 804, and 807
d) Is the ESI an original or duplicate (Original writing rule) and, if not, is their secondary evidence that can prove the content of the ESI? FRE 1001-1008
e) Does the probative value of the ESI outweigh any prejudicial effect? FRE 403.

3) Relevance—FRE 401

a) Judge makes preliminary determination under FRE 104(a). FRE does not apply except for privilege issues.[9]
b) "In essence, determining whether ESI is authentic, and therefore relevant, is a two step process. First, before admitting evidence for consideration by the jury, the district court must determine whether its proponent has offered a satisfactory foundation from which the jury could reasonably find that the evidence is authentic. Then, because authentication is essentially a question of conditional relevancy, the jury ultimately resolves whether evidence admitted for its consideration is that which the proponent claims."[10]
c) "For 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 a 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."[11]
d) Irrelevant evidence is inadmissible.[12] But once evidence is shown to be relevant, it is presumptively admissible unless barred by another rule of law.[13]

[8] *Id*. at 538.
[9] *Id*. at 539.
[10] *Id*. at 539-40 (citations omitted).
[11] *Id*. at 540.
[12] *Id*. at 541.
[13] *Id*. at 541.

4) Authentication—FRE 901(a)

"[T]here is no single approach to authentication that will work in all instances."[14]

a) "The Requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."[15]
b) "A party seeking to admit an exhibit need only make a prima facie showing that it is what he or she claims it to be."[16]
c) Failure to get evidence admitted is almost always "a self inflicted injury which can be avoided by thoughtful advance preparation."[17]
d) "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."[18]
e) FRE 901(b) sets forth examples of authentication/identification that conform to Rule 901(a).
    i) FRE 901(b)(1): "*Testimony of Witness With Knowledge.* Testimony that a matter is what it is claimed to be."
        (1) "Courts considering the admissibility of electronic evidence frequently have acknowledge that it may be authenticated by a witness with personal knowledge."[19]
            (a) Authentication of computer records by custodian or qualified witness with personal knowledge.[20]
            (b) Authentication of website printouts from webmaster.[21]
            (c) *Cf.* evidence not admissible where affiant did not have personal knowledge.[22]
        (2) Authentication may occur if the witness has personal knowledge about how an exhibit is routinely made.
            (a) "Although Rule 901(b)(1) certainly is met by the testimony of a witness that actually drafted the exhibit, it is not required that the authenticating witness have personal knowledge of the making of a particular exhibit if he or she has personal knowledge of how that type of exhibit is routinely made. It is necessary, however, that the authenticating witness provide factual specificity about the process by

[14] *Id*. at 554.
[15] FRE 901(a).
[16] *Markel,* 241 F.R.D. at 542.
[17] *Id*. at 543.
[18] *Id* at 544 (citation omitted).
[19] *Id*. at 545.
[20] *Id*. at 545.
[21] *Id*. at 545.
[22] *Id.* at 545.

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, as opposed to boilerplate, conclusory statements that simply parrot the elements of the business record exception to the hearsay rule, Rule 803(6), or public record exception, Rule 803(8)."[23]

f) FRE 901(b)(3): "*Comparison by Trier or Expert Witness*. Comparison by the trier of fact or by expert witnesses with specimens which have been authenticated."
   i) "E-mail messages that are not clearly identifiable on their own can be authenticated ... by comparison by the trier of fact (the jury) with specimens which have been [otherwise] authenticated-in this case, those e-mails that already have been independently authenticated under Rule 901(b)(4)."[24]

g) FRE 901(b)(4): "*Distinctive Characteristics and the Like.* Appearance, contents, substance, internal patters, or other distinctive characteristics, taken in conjunction with circumstances."
   i) "Courts have recognized this rule as a means to authenticate ESI, including e-mail, text messages and the content of websites."[25]
      (1) Authentication permissible through circumstantial evidence such as person's email address, content of message that is related to other admissible evidence (including use of person's name).[26]
      (2) Authentication of website printout through printed date and website address.[27]
   ii) Authentication through hash values/marks
      (1) "A unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. The most commonly used algorithms, known as MD5 and SHA, will generate numerical values so distinctive that the chance that any two data sets will have the same hash value, no matter how similar they appear, is less than one in one billion. 'Hashing' is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production. "[28]
      (2) "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 of electronic records to create a form of electronic 'Bates stamp' that will help establish the document as electronic."[29]

---

[23] *Id.* at 545-46.
[24] *Id*. at 546 (citations omitted).
[25] *Id*. at 546.
[26] *Id*. at 546.
[27] *Id*. at 546.
[28] *Id*. at 546-47 (*citing* Federal Judicial Center, *Managing Discovery of Electronic Information: A Pocket Guide for Judges,* Federal Judicial Center, 2007 at 24).
[29] *Id*. at 547.

(3) "Use of hash values when creating the 'final' or 'legally operative' version of an electronic record can insert distinctive characteristics into it that allow its authentication under Rule 901(b)(4)."[30]

iii) Authentication through metadata (i.e., data about data).

(1) Metadata has been defined as "information about a particular data set which describes how, when and by whom it was collected, created, accessed, or modified and how it is formatted (including data demographics such as size, location, storage requirements and media information)."[31]

(2) A party may request production of ESI in its native format which will include the metadata.[32]

(3) "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 a distinctive characteristic of all electronic evidence that can be used to authenticate it under Rule 901(b)(4)."[33]

(4) *Warning:* Relying upon metadata is not a foolproof method of authentication. ESI can be accessed (either intentionally or unintentionally) which can result in the metadata being changed.[34]

h) FRE 901(b)(7): "*Public Records or Reports.* Evidence that a writing authorized by law to be recorded or filed and in fact recorded or filed in a public office, or a purported public record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept."

i) "To use this rule the 'proponent of the evidence need only show that the office from which the records were taken is the legal custodian of the records.'…. Examples of the types of public records that may be authenticated by Rule 901(b)(7) include 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, and data compilations, which may include computer stored records."[35]

ii) "Courts have recognized the appropriateness of authenticating computer stored public records under Rule 901(b)(7) as well, and observed that under this rule, unlike Rule 901(b)(9), there is no need to show that the computer system producing the public records was reliable or the records accurate."[36]

iii) *Remember:* There are multiple ways to authenticate evidence. It may be easier to authenticate under one rule than another.[37]

---

[30] *Id*. at 547.
[31] *Id*. at 547 (*citing* Appendix F to *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age*).
[32] *Id*. at 547.
[33] *Id*. at 547-48.
[34] *Id*. at 548.
[35] *Id*. at 549 (citation omitted).
[36] *Id*. at 548.
[37] *Id*. at 548-49.

i) FRE 901(b)(9): "*Process of System.* Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result."
   i) This rule was intended for computer generated evidence.[38]

j) FRE 902—Self-Authentication
   i) General pointers:
      (1) "The obvious advantage of Rule 902 is that it does not require the sponsoring testimony of any witness to authenticate the exhibit-its admissibility is determined simply by examining the evidence itself, along with any accompanying written declaration or certificate required by Rule 902. The mere fact that the rule permits self-authentication, however, does not foreclose the opposing party from challenging the authenticity."[39]
   ii) FRE 902(5): "Official Publications. Books, pamphlets, or other publications purporting to be issued by public authority."
      (1) "Given the frequency with which official publications from government agencies are relevant to litigation and the increasing tendency for such agencies to have their own websites, Rule 902(5) provides a very useful method of authenticating these publications. When combined with the public records exception to the hearsay rule, Rule 803(8), these official publications posted on government agency websites should be admitted into evidence easily."[40]
      (2) Example of rule application: admission of website postings from official government agency.[41]
   iii) FRE 902(7): "Trade Inscriptions and the Like. Inscriptions, signs, tags or labels purporting to have affixed in the course of business and indicating ownership, control, or origin."
      (1) "As one commentator has noted, '[u]nder Rule 902(7), labels or tags affixed in the course of business require no authentication. 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).'"[42]
   iv) FRE 902(11) provides:

> (11) Certified domestic records of regularly conducted activity. The original or a duplicate of a domestic record of regularly conducted activity that would be admissible under Rule 803(6) if accompanied by a written declaration of its custodian or other qualified person, in a manner complying with any Act of Congress or rule prescribed by the Supreme Court pursuant to statutory authority, certifying that the record:

---

[38] *Id*. at 549.
[39] *Id*. at 551.
[40] *Id*. at 551.
[41] *Id*. at 551.
[42] *Id.* at 551-52 (*citing* Jack B. Weinstein & Margaret A. Berger, *Weinstein's Federal Evidence* § 900.07 [3] (Joseph M. McLaughlin ed., Matthew Bender 2d ed.1997)(hereinafter "WEINSTEIN")).

(A) was made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;

(B) was kept in the course of the regularly conducted activity; and

(C) was made by the regularly conducted activity as a regular practice.

A party intending to offer a record into evidence under this paragraph must provide written notice of that intention to all adverse parties, and must make the record and declaration available for inspection sufficiently in advance of their offer into evidence to provide an adverse party with a fair opportunity to challenge them.

v) Rule 902(11) has the same elements as FRE 803(6) and hence authenticity is often analyzed under both rules.[43]

k) Other methods to authenticate documents
   i) Be creative—Think "outside the box."[44]
      (1) Courts "have held that 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."[45]
      (2) "Defendants cannot have it both ways. They cannot voluntarily produce documents and implicitly represent their authenticity and then contend they cannot be used by the Plaintiffs because the authenticity is lacking."[46]
   ii) FRE 201—Judicial Notice of Adjudicative Facts
      (1) "A judicially noticed fact must be one not subject to reasonable dispute in that it is either (1) generally known within the territorial jurisdiction of the trial court or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." FRE 201(b).
   iii) Fed. R. Civ. P. 36—Request for admission that a document is genuine/authentic.
   iv) Fed. R. Civ. P. 16(c)(3)—Stipulation at pre-trial conference regarding authentication of documents
   v) Fed. R. Civ. P. 26(a)(3)
      (1) "[I]f a party properly makes his or her FED. R. CIV. P. 26(a)(3) pretrial disclosures of documents and exhibits, then the other side has fourteen days in which to file objections. Failure to do so waives all objections other than under Rules 402 or 403, unless the court excuses the waiver for

[43] *Id.* at 552.
[44] *Id.* at 552.
[45] *Id.* at 552.
[46] *Id.* at 553 (citation omitted).

good cause. This means that if the opposing party does not raise authenticity objections within the fourteen days, they are waived."[47]

vi) Depositions—a party may authenticate a document via deposition testimony later introduced as evidence.[48]

5) Hearsay and Exceptions—FRE 801-802, 804, 807

a) General methodology for analyzing hearsay:
   i) "(1) does the evidence constitute a **statement,** as defined by Rule 801(a); (2) was the statement made by a "**declarant,**" as defined by Rule 801(b); (3) is the statement being offered to prove the **truth of its contents,** as provided by Rule 801(c); (4) is the statement **excluded from the definition of hearsay by rule 801(d);** and (5) if the statement is hearsay, is it covered by one of the exceptions identified at Rules 803, 804 or 807."[49]

b) Is it a statement? "A 'statement' is (1) an oral or written assertion or (2) nonverbal conduct of a person, if it is intended by the person as an assertion."[50]

c) Was the statement made by a declarant? "A 'declarant' is a person who makes a statement."[51]
   i) "When an electronically generated record is entirely the product of the functioning of a computerized system or process, such as the 'report' generated when a fax is sent 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. For that reason, the record is not a statement and cannot be hearsay."[52]
   ii) "Where the writings are non-assertive, or not made by a 'person,' courts have held that they do not constitute hearsay, as they are not 'statements.'"[53]
      (1) Fax header not hearsay.[54]
      (2) Images/text posted on website not hearsay.[55]

d) Is the statement hearsay? "'Hearsay' is a statement…offered in evidence to prove the truth of the matter asserted."[56]
   i) "When analyzing the admissibility of electronically generated evidence, courts also have held that statements contained within such evidence fall outside the hearsay definition if offered for a purpose other than their substantive truth."[57]

---

[47] *Id*. at 553 (emphasis added).
[48] *Id*. at 582.
[49] *Id*. at 562-63 (bold in original).
[50] FRE 801(a).
[51] FRE 801(b).
[52] *Markel,* 241 F.R.D. at 564.
[53] *Id.* at 564.
[54] *Id.* at 564
[55] *Id*. at 565.
[56] FRE 801(c).
[57] *Markel,* 241 F.R.D. at 566

ii) "[C]ommunications between the parties to a contract that define the terms of a contract, or prove its content, are not hearsay, as they are verbal acts or legally operative facts. "[58]

iii) It is critical to remember that in offering evidence, a party must articulate the non-hearsay basis for admissibility.[59]

e) Is the statement not hearsay under FRE 801(d)(1) or (d)(2)?

i) FRE 801(d) provides:

(d) Statements which are not hearsay.

A statement is not hearsay if--

> (1) *Prior statement by witness*. The declarant testifies at the trial or hearing and is subject to cross-examination concerning the statement, and the statement is (A) inconsistent with the declarant's testimony, and was given under oath subject to the penalty of perjury at a trial, hearing, or other proceeding, or in a deposition, or (B) consistent with the declarant's testimony and is offered to rebut an express or implied charge against the declarant of recent fabrication or improper influence or motive, or (C) one of identification of a person made after perceiving the person; or
>
> (2)*Admission by party-opponent.* The statement is offered against a party and is
>
> > (A) the party's own statement, in either an individual or a representative capacity or
> >
> > (B) a statement of which the party has manifested an adoption or belief in its truth, or
> >
> > (C) a statement by a person authorized by the party to make a statement concerning the subject, or
> >
> > (D) a statement by the party's agent or servant concerning a matter within the scope of the agency or employment, made during the existence of the relationship, or
> >
> > (E) a statement by a coconspirator of a party during the course and in furtherance of the conspiracy.

The contents of the statement shall be considered but are not alone sufficient to establish the declarant's authority under subdivision (C), the agency or employment relationship and scope thereof under subdivision

[58] *Id*. at 566.
[59] *Id*. at 567.

(D), or the existence of the conspiracy and the participation therein of the declarant and the party against whom the statement is offered under subdivision (E).

ii) Examples of non-hearsay
(1) Defendant's email constitutes an admission.[60]
(2) Defendant's website admissible against defendant.[61]

f) If the statement is hearsay, is there an exception under FRE 803, 804, or 807?
i) The *Markel* decision succinctly articulates how FRE 803 can be broken down into three broad categories:

> Rule 803 may be grouped in three broad categories: **Category 1** includes exceptions dealing with **perceptions, observations, state of mind, intent and sensation** 803(1) (present sense impressions); 803(2) (excited utterances); 803(3) (then existing state of mind, condition or sensation); 803(4) (statements in furtherance of medical diagnosis and treatment). **Category 2** includes **documents, records, and other writings** 803(5) (past recollection recorded); 803(6) & (7) (business records); 803(8) & (10) (public records); 803(9) (records of vital statistics); 803(11) (records of religious organizations); 803(12) (certificates of baptism, marriage and related events); 803(13) (family records); 803(14) (records of documents affecting an interest in property); 803(15) (statements in documents affecting an interest in property); 803(16) (ancient documents); 803(18) (learned treatises); 803(22) (judgments of conviction in a criminal case); and 803(23) (judgments in certain kinds of civil cases). **Category 3** includes statements dealing with **reputation** 803(19) (reputation regarding personal or family history); 803(20) (reputation regarding custom, use and practice associated with land, and historically significant facts); and 803(21) (reputation regarding character within the community and among associates).[62]

ii) FRE 803(1) Present Sense Impression—"A statement describing or explaining an event or condition made while the declarant was perceiving the event or condition, or immediately thereafter."
(1) "There are three elements that must be met for this hearsay exception to apply: (1) the declarant must have personally perceived the event that is described in the statement; (2) the statement must be a simple explanation or description of the event perceived; and (3) the declaration and the event described must be contemporaneous."[63]

---

[60] *Id*. at 568.
[61] *Id*. at 568.
[62] *Id*. at 568 (emphasis in original).
[63] *Id*. at 569.

iii) FRE 803(2) Excited Utterance—"A statement relating to a startling event or condition made while the declarant was under the stress of excitement caused by the event or condition."

iv) FRE 803(3) Then Existing Mental, Emotional or Physical Condition

(1) "The foundation for proving an exception under Rule 803(3) is: (1) The statement must be contemporaneous with the mental state being proven; (2) There must be [an absence of] suspicious circumstances that would evidence a motive for fabrication or misrepresentation of the declarant's state of mind; and (3) The state of mind of the declarant must be relevant in the case."[64]

(2) Critically, it must be noted that "Rule 803(3) has been used to prove a wide variety of matters, including the reason why the declarant would not deal with a supplier or dealer, motive, competency, ill-will, motive, lack of intent to defraud, willingness to engage in criminal conduct, the victim's state of mind in an extortion case, and confusion or secondary meaning in a trademark infringement case."[65]

v) FRE 803(6) Records of Regularly Conducted Activity

(1) FRE 803(6) provides:

> (6) **Records of regularly conducted activity.** A memorandum, report, record, or data compilation, in any form, of acts, events, conditions, opinions, or diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation, all as shown by the testimony of the custodian or other qualified witness, or by certification that complies with Rule 902(11), Rule 902(12), or a statute permitting certification, unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

(2) "The foundational elements for a business record are: (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 events it records; (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; and (4) to have been made in the normal course of business means that the document was made in the regular course of a regularly conducted business activity, for which it was the regular practice of the business to maintain a memorandum."[66]

---

[64] *Id*. at 570 (*citing* WEINSTEIN at § 803.05[2][a]).
[65] *Id*. at 570.
[66] *Id*. at 571.

(3) Remember, business records can be self-authenticated if the elements of Rule 902(11) can be shown.
(4) Remember, that However, "[i]f the source of the information is an outsider, Rule 803(6) does not, by itself, permit the admission of the business record. The outsider's statement must fall within another hearsay exception to be admissible because it does not have the presumption of accuracy that statements made during the regular course of business have."[67]
(5) "To satisfy Rule 803(6) each participant in the chain which created the record-from the initial observer-reporter to the final entrant-must generally be acting in the course of the regularly conduct[ed] business. If some participant is not so engaged, some other hearsay exception must apply to that link of the chain."[68]
(6) Remember, courts apply differing levels of standards. Some such as *Vinhnee* will require a showing that "outputted" data is the same as the "inputted" data. This can be a difficult burden to overcome. Other courts will be less stringent and find that ESI created at the time of the transaction is admissible.[69]

vi) FRE 803(8)—Public Records and Reports—"Records, reports, statements, or data compilations, in any form, of public offices or agencies, setting forth (A) the activities of the office or agency, or (B) matters observed pursuant to duty imposed by law as to which matters there was a duty to report, excluding, however, in criminal cases matters observed by police officers and other law enforcement personnel, or (C) in civil actions and proceedings and against the Government in criminal cases, factual findings resulting from an investigation made pursuant to authority granted by law, unless the sources of information or other circumstances indicate lack of trustworthiness."
(1) Courts tend to apply a "deferential standard of admissibility for electronic public records."[70]
(2) Examples
(a) UCC financing statements
(b) Real estate recordings

vii) FRE 803(17)—Market Reports, Commercial Publications—"Market quotations, tabulations, lists, directories, or other published compilations, generally used and relied upon by the public or by persons in particular occupations."
(1) Examples
(a) Wall Street Journal
(b) Kelley Blue Book

viii) *Remember:* "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."[71]

---

[67] *Id*. at 572 (citation omitted).
[68] *Id.* at 573 (citation omitted).
[69] *Id*. at 573-74.
[70] *Id*. at 574-75.

6) Original Writing Rule—FRE 1001-1008

a) FRE 1002—Requirement of Original—"To prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress."
   i) "[T]he key to the rule is to determine when 'the contents' of a writing, recording or photograph actually are being proved, as opposed to proving events that just happen to have been recorded or photographed, or those which can be proved by eyewitnesses, as opposed to a writing or recording explaining or depicting them."[72]

b) Rule 1003—"Admissibility of Duplicates"—"A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original."

c) Rule 1005—"Public Records"—"The contents of an official record, or of a document authorized to be recorded or filed and actually recorded or filed, including data compilations in any form, if otherwise admissible, may be proved by copy, certified as correct in accordance with rule 902 or testified to be correct by a witness who has compared it with the original. If a copy which complies with the foregoing cannot be obtained by the exercise of reasonable diligence, then other evidence of the contents may be given."

d) Rule 1006—"Summaries"—"The contents of voluminous writings, recordings, or photographs which cannot conveniently be examined in court may be presented in the form of a chart, summary, or calculation. The originals, or duplicates, shall be made available for examination or copying, or both, by other parties at reasonable time and place. The court may order that they be produced in court."
   i) "Rule 1006 permits introduction into evidence of written or testimonial summaries of voluminous writings, recordings or photographs, provided the original or duplicates from which the summaries were prepared were made available to the adverse party at a reasonable time in advance of trial for examination or copying."[73]
   ii) "Because 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."[74]

e) One commentator has succinctly stated the relationship regarding the Original Writing Rule and ESI:

> ***Computer-based business records commonly consist of material originally produced in a computer (e.g. business memoranda), data drawn from outside sources and input into the computer (e.g. invoices), or summaries of documents (e.g. statistical runs). The admissibility of computer-based records 'to prove the content of a***

---

[71] *Id*. at 575.
[72] *Id*. at 576.
[73] *Id*. at 576
[74] *Id*. at 581.

writing' is subject to the best evidence rule set out in Rule 1002. The rule generally requires the original of a writing when the contents are at issue, except that a 'duplicate' is also admissible unless a genuine issue is raised about its authenticity. A duplicate includes a counterpart produced by 'electronic re-recording, which accurately reproduces the original.' Courts often admit computer-based records without making the distinction between originals and duplicates.[75]

f) "When analyzing the original writing rule as it applies to electronic evidence, the most important rules are Rule 1001, containing the definitions; Rule 1002, the substantive original writing rule; Rule 1004, the 'primary' secondary evidence rule; Rule 1006, the rule permitting summaries to prove the contents of voluminous writings, recordings and photographs; and Rule 1007, allowing proof of a writing, recording or photograph by the admission of a party opponent."[76]
g) Other points
   i) "It is important to keep in mind that failure to properly object to the introduction of evidence in violation of the original writing rule likely will result in a waiver of the error on appeal."[77]
   ii) "Counsel need to insure that a timely objection is made to attempts to prove the contents of electronic writings, recordings or photographs in violation of the original writing rule, otherwise waiver of the error is the probable consequence."[78]

7) Probative Value/Prejudicial Effect—FRE 403

a) Rule 403—Exclusion of Relevant Evidence on Grounds of Prejudice, Confusion, or Waste of Time—"Although relevant, evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence."
b) Examples
   i) Evidence contains language that will evoke a deep emotional response.[79]
   ii) Confusing computer animations for reality.[80]

"Because it can be expected that electronic evidence will constitute much, if not most, of the evidence used in future motions practice or at trial, counsel should know how to get it right on the first try."[81]

---

[75] *Id*. at 577 (citing WEINSTEIN at § 900.07[1][d][iv]).
[76] *Id*. at 577.
[77] *Id*. at 579.
[78] *Id*. at 579.
[79] *Id*. at 584.
[80] *Id*. at 584.
[81] *Id*. at 585.

Part II:
Application of Rules to Different Types of ESI

8) Overview of Test:

a) "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 (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 Rule 901(a) (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, of 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, such that it should be excluded despite its relevance."[82]

9) Email

a) General Points:
   i) "Perhaps because of the spontaneity and informality of e-mail, people tend to reveal more of themselves, for better or worse, than in other more deliberative forms of written communication. For that reason, e-mail evidence often figures prominently in cases where state of mind, motive and intent must be proved."[83]

b) Admissibility test
   i) Relevant?
   ii) Authentic?
   iii) Hearsay—Exception?
   iv) Original Writing?
   v) Unfair Prejudice?

c) Authentication
   i) *Markel* sets forth numerous ways by which email may be authenticated:[84]

> [E]-mail messages may be authenticated by direct or circumstantial evidence. An e-mail message's distinctive characteristics, including its 'contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances' may be sufficient for authentication.

[82] *Id*. at 538
[83] *Id*. at 554.
[84] *Id*. at 554 (citing Weinstein at § 900.07[3][c])

> Printouts 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.
>
> The contents of the e-mail may help show authentication by revealing details known only to the sender and the person receiving the message.
>
> E-mails may even be self-authenticating. Under Rule 902(7), labels or tags affixed in the course of business require no authentication. 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. For example, a person with unauthorized access to a computer can transmit e-mail messages under the computer owner's name. Because of the potential for unauthorized transmission of e-mail messages, authentication requires testimony from a person with personal knowledge of the transmission or receipt to ensure its trustworthiness."

   ii) "The most frequent ways to authenticate e-mail evidence are 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)."[85]

d) Hearsay
   i) Given the spontaneity of emails, it may be a fertile source to fit within the hearsay of exceptions of present sense impression[86] or excited utterance.[87]
   ii) Does an email qualify as a business record?

10) Internet Website Postings

a) Admissibility test
   i) Relevant?
   ii) Authentic?
   iii) Hearsay—Exception?
   iv) Original Writing?

---

[85] *Id*. at 555.
[86] FRE 803(1).
[87] FRE 803(2).

v) Unfair Prejudice?

b) Authentication
   i) "In applying [the authentication standard] to website evidence, there are three questions that must be answered explicitly or implicitly. (1) What was actually on the website? (2) Does the exhibit or testimony accurately reflect it? (3) If so, is it attributable to the owner of the site?"[88]
   ii) "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)."[89]

11) Text Messages and Chat Room Content

a) Admissibility test
   i) Relevant?
   ii) Authentic?
   iii) Hearsay—Exception?
   iv) Original Writing?
   v) Unfair Prejudice?

b) "[T]he rules most likely to be used to authenticate chat room and text messages, alone or in combination, appear to be 901(b)(1) (witness with personal knowledge) and 901(b)(4) (circumstantial evidence of distinctive characteristics)."[90]

12) Computer Stored Records and Data (e.g., Database ESI)

a) General Points
   i) "[A]lthough computer records are the easiest to authenticate, there is growing recognition that more care is required to authenticate these electronic records than traditional 'hard copy' records."[91]

b) Admissibility test
   i) Relevant?
   ii) Authentic?
   iii) Hearsay—Exception?
   iv) Original Writing?
   v) Unfair Prejudice?

c) Differing standards of leniency for admissibility
   i) Lenient standard
      (1) Computer records authenticated as business records where custodian confirmed the Rule 803(6) elements were met.[92]

---

[88] *Markel,* 241 F.R.D. at 555 (citing Gregory P. Joseph, *Internet and Email Evidence,* 13 Prac. Litigator (Mar.2002), *reprinted in* 5 Stephen A. Saltzburg et al., Federal Rules of Evidence Manual, Part 4 at 21 (9th ed.2006)).
[89] *Id*. at 556.
[90] *Id*. at 556.
[91] *Id*. at 557.
[92] *Id*. at 557.

(2) Electronic bill of lading properly admitted where only foundation evidence was that record was created at the time the parties entered into their contract.[93]

ii) Stringent standard: *In re Vee Vinhnee*, 336 B.R. 437 (9th Cir. BAP 2005).

(1) Adopted a slightly modified 11-step foundational approach advocated by Edward J. Imwinkelried, *Evidentiary Foundations* § 403[2] (5th ed. 2002).

(a) Imwinkelried's foundational steps are:

> 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.[94]

iii) What approach should you use?

> ***"If it is critical to the success of your case to admit into evidence computer stored records, it would be prudent to plan to authenticate the record by the most rigorous standard that may be applied."***[95]

d) "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)."[96]

e) Key pointers in dealing with "database" ESI

i) Given the widespread use databases in commercial operations and given relatively volatile state of the ESI, it behooves a practitioner to have a good game plan when dealing with database ESI in a litigation context.

---

[93] *Id*. at 557.
[94] *Id*. at 558 (*citing Vinhnee*, 336 B.R. at 446-47).
[95] *Id. at 559.*
[96] *Id*. at 559.

ii) The following recommendations are based upon electronic discovery technical and legal practice experience of Fios Inc.:[97]

> The potentially dynamic and volatile state of a database can add levels of complexity to the already complex matter of ESI preservation and authentication. The following is a "highlights" list of considerations when looking to defensibly preserve database ESI.
>
> 1. Identify and inventory the existing databases that may contain potentially relevant ESI (ESI Content Mapping). Document key personnel and their long term contact info so they may be located in the future.
> 2. It is very important to talk with a database expert and the application owner to determine an optimal preservation plan.
> 3. Identify governance practices, including auto-purging of data (e.g., data that is discarded after a set period of time, or ad hoc processes that delete information when storage space becomes an issue) and retention policies.
> 4. Identify replication practices, including if the data is being routinely backed up for business continuity, how long tapes are retained, and if the data is replicated to other repositories (e.g., data warehouses that may be easier to access).
> 5. Identify preservation capabilities, including how routine destruction or purging can be suspended and if records can be preserved in place or much be collected to be preserved;
>   a. Small databases can be copied periodically to make a complete "backup"
>   b. Larger databases can be backed up using "block backup" software—the large database is preserved and the small blocks of changed data are preserved, saving space and time. The downside of this method is additional time required to reconstruct a given "point in time" on the database.
> 6. Identify collection or extraction capabilities. Once data has been preserved, how it is accessed, queried and extracted and/or reported.

[97] Expertise provided by Mary Mack, Esq. and Brad Harris and synthesized by Aaron Cronan, Esq. Fios is a Socha-Gelbmann "Top 5" electronic discovery services provider exclusively focused on delivering comprehensive services and expert guidance throughout all phases of the litigation process. The company may be contacted at Fios, Inc. c/o Aaron Cronan, Esq., 921 SW Washington St., Suite 850, Portland, Oregon 97205, (503) 808-1614, acronan@fiosinc.com

7. Present a reasonable preservation plan to opposition as soon as possible. Seek costs for doing more and/or court blessing of the plan. Do not wait for the meet and confer.

13) Computer Animation and Computer Simulations

a) Admissibility test
   i) Relevant?
   ii) Authentic?
   iii) Hearsay—Exception?
   iv) Original Writing?
   v) Unfair Prejudice?
b) Authentication
   i) "[T]he most frequent methods of authenticating computer animations are 901(b)(1) (witness with personal knowledge), and 901(b)(3) (testimony of an expert witness)."[98]
   ii) "[T]he most frequent methods of authenticating computer simulations are 901(b)(1) (witness with personal knowledge); and 901(b)(3) (expert witness). Use of an expert witness to authenticate a computer simulation likely will also involve Federal Rules of Evidence 702 and 703."[99]
c) Unfairly Prejudicial—One key concern is that people may give more weight/credibility to a computer simulation or model.

14) Digital Photographs

a) Admissibility test
   i) Relevant?
   ii) Authentic?
   iii) Hearsay—Exception?
   iv) Original Writing?
   v) Unfair Prejudice?
b) Three types of digital photographs:
   i) Original digital images—authenticated by a witness with personal knowledge.[100]
   ii) Digitally converted images—authenticated with explanation as to who the process properly converted the image.[101]
   iii) Digitally enhanced images—"there will need to be proof, permissible under Rule 901(b)(9), that the digital enhancement process produces reliable and accurate results, which gets into the realm of scientific or technical evidence under Rule 702."[102]

[98] *Markel,* 241 F.R.D. at 560.
[99] *Id*. at 560-61.
[100] *Id*. at 561.
[101] *Id.* at 561.
[102] *Id*. at 561.