LORRAINE v. MARKEL AMER. INS. CO.
UNITED STATES DISTRICT COURT FOR THE DISTRICT OF MARYLAND
241 F.R.D. 534 (2007)

MEMORANDUM OPINION

Plaintiffs/ Counter-Defendants Jack Lorraine and Beverly Mack bring this action to enforce a private arbitrator's award finding that certain damage to their yacht, Chessie, was caused by a lightning strike that occurred on May 17, 2004, while Chessie was anchored in the Chesapeake Bay. Defendant/ Counter-Plaintiff Markel American Insurance Company ("Markel") likewise has counterclaimed to enforce the arbitrator's award, which, in addition to concluding that certain damage to Chessie's hull was caused by lightning, also concluded that the damage incurred was limited to an amount of $14,100, plus incidental costs. Following discovery, Plaintiffs moved for summary judgment (Paper No. 16), and Defendants filed a response in opposition and cross motion for summary judgment (Paper No. 19), to which Plaintiffs filed an opposition and reply (Paper No. 21), followed by Defendant's reply (Paper No. 23). In a letter order dated February 7, 2007 (Paper No. 26), I denied without prejudice both motions for the reasons discussed more fully below, and informed the parties that I intended to file a more comprehensive opinion explaining my ruling, which is found herein.

BACKGROUND

It is difficult for the Court to provide the appropriate background to the underlying arbitration in this case because, as will be discussed in greater detail below, neither party has proffered any admissible evidence to support the facts set forth in their respective motions. See *FED. R. CIV. P. 56(c)*. Based on the pleadings, however, it appears undisputed that Chessie was struck by lightning on May 17, 2004, and that Plaintiffs filed a claim with Markel, their insurance carrier, for certain damage incurred as a result of the strike. Compl. PP 5, 6; Answer PP 2, 6. Markel issued payment under the policy for some of the damage claimed, and the matter would have been concluded had Plaintiffs not discovered damage to the hull when they pulled the boat out of the water several months later. Compl. P 7. Markel denied that the hull damage was caused by the lightning strike and/or covered by Plaintiffs' insurance policy, and initiated a declaratory judgment action in the United States District Court for the Middle District of Pennsylvania to that effect. Compl. P 13, Answer P 15. The parties subsequently negotiated a private arbitration agreement and voluntarily dismissed the Pennsylvania claim. Compl. P 15, Answer P 17.

The scope of the arbitration agreement is the basis of this litigation. The final agreement states, in relevant part,

> The parties to this dispute . . . have agreed that an arbitrator shall determine whether certain bottom damage in the amount of $36,000, to the Yacht CHESSIE was caused by the lightning strike occurring on May 17, 2004, or osmosis, as claimed by [Markel]. Pl.'s Mot. Ex. A, Def.'s Mot. Ex. C. The agreement also contemplated that the arbitrator would issue an "award" within 30 days of the final submission of evidence. Id. The arbitrator issued his

award on June 12, 2006. In it, he held that some, but not all, of Chessie's hull damage was caused by lightning. Specifically, the arbitrator stated,

> I find that there is a basis for an argument regarding loss related damage. Evidence shows that the lightning strike on Mary 17, 2004 was discharged through the hull below the water line . . . . The corruption of the surface laminate of the bottom is basis for a loss related award . . . . The award amount must be kept in proportion to the loss related damage only. I find that the repairs relating to that damage should be based on a cost of $300.00 per foot ($14,000.00). Other expenses relating to charges for hauling, mast un-stepping/re-stepping, blocking, storage, moving, launching or environmental fees should be added to that amount.

Def.'s Mot. Ex. D. This award forms the basis for the present litigation, in which both parties ostensibly seek to confirm and enforce the arbitrator's decision.

SUMMARY JUDGMENT STANDARD

Summary judgment is appropriate when there exists no genuine issue as to any material fact and a decision may be rendered as a matter of law. *Fed. R. Civ. P. 56(c)*; *Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 247, 106 S. Ct. 2505, 91 L. Ed. 2d 202 (1986)*. The party moving for summary judgment has the burden of demonstrating that there are no genuine issues of material facts to resolve. *Pulliam Inv. Co. v. Cameo Properties, 810 F.2d 1282, 1286 (4th Cir. 1987)*. In determining whether summary judgment should be granted, the court "must assess the documentary materials submitted by the parties in the light most favorable to the nonmoving party." Id. (citing *Gill v. Rollins Protective Services Co., 773 F.2d 592, 598 (4th Cir. 1985))*. * * * To be entitled to consideration on summary judgment, the evidence supporting the facts set forth by the parties must be such as would be admissible in evidence. See *FED. R. CIV. P. 56(c).* * * *. With regard to documentary evidence, this Court previously has held that,

> [u]nsworn, unauthenticated documents cannot be considered on a motion for summary judgment. To be admissible at the summary judgment stage, documents must be authenticated by and attached to an affidavit that meets the requirements of *Rule 56(e)*-that the documents be admissible in evidence.

Miskin v. Baxter Healthcare Corp. et al., 107 F. Supp. 2d 669 (D. Md. 1999) (Grimm, J.) (citing *Orsi v. Kirkwood, 999 F.2d 86, 92 (4th Cir. 1993)*.

THE FEDERAL ARBITRATION ACT

As a preliminary matter, Plaintiffs have styled their complaint as one to enforce the arbitrator's award under *§ 9* of the Federal Arbitration Act, *9 U.S.C. § 1 et seq. (2006)*, when, in reality, it is a complaint to modify the award under *section 10* of that statute. This is so because, although the arbitrator found that only $14,100 of Chessie's hull damage was caused by lightning, Plaintiffs nonetheless ask the Court to award a judgment in the amount of $36,000. Plaintiffs' argument regarding the substance of the agreement between the parties further underscores this conclusion. Specifically, Plaintiffs allege that the parties entered into an "all or nothing" agreement, whereby

the arbitrator was to determine that the hull damage was caused by lightning, and if so, award Plaintiffs the $36,000.00 in damages claimed. Pl.'s MSJ at 5. According to Plaintiffs,

> the Arbitrator's sole function was to determine whether the hull damage, in the agreed-upon amount of $36,000, was caused by the lightning strike occurring on May 17, 2004. The Arbitration Agreement did not grant the Arbitrator the authority to assess a damage amount.

Id. (emphasis added). This argument is consistent with a motion to modify under *§ 10(a)(4)*, which permits a federal court to modify or vacate an arbitration award upon a showing that "the arbitrator[] exceeded their powers." Accordingly, the Court will evaluate Plaintiffs' motion under *§ 10 of the FAA*.

In contrast, Markel's complaint truly is one to enforce the arbitrator's award. Markel denies that it entered into an "all or nothing" arbitration agreement with regard to damages, and seeks to enforce the arbitrator's award of $14,100. Def.'s Mot. at 5.

The question before the Court, therefore, is whether the arbitrator exceeded his authority under the arbitration agreement by assigning a value to the damages attributable to the lightning strike that was less than the $36,000 claimed by Plaintiffs. If the answer is yes, then the court can vacate, remand, or modify the award. *9 U.S.C. § 10*, *11*. If the answer is no, then the court must grant Defendant's motion to confirm the award under *§ 9 of the FAA*.

To resolve whether the arbitrator exceeded his authority, the Court first must determine the scope of the arbitration agreement; specifically, whether the parties agreed to arbitrate the amount of damages caused by the lightning strike. Because the parties did not agree to submit questions of arbitrability to the arbitrator for resolution, determining the scope of the agreement is an issue for the Court to decide. *First Options of Chicago, Inc. v. Kaplan, 514 U.S. 938, 943, 115 S. Ct. 1920, 131 L. Ed. 2d 985 (1995)*. In this regard, the Supreme Court has advised that, "[w]hen deciding whether the parties agreed to arbitrate a certain matter . . . courts generally . . . should apply ordinary state-law principles of contract interpretation." *Kaplan, 514 U.S. at 944*, accord *E.I. Dupont De Nemours & Co. v. Martinsville Nylon Employees' Council Corp., 78 F.3d 578 (4th Cir. 1996)*. In doing so, the Court must "give due regard to the federal policy favoring arbitration and resolve 'any doubts concerning the scope of arbitrable issues in favor of arbitration." *Hill v. PeopleSoft USA, Inc., 412 F.3d 540, 543 (4th Cir. 2005)* (quoting *Moses H. Cone Mem'l Hosp. v. Mercury Constr. Corp., 460 U.S. 1, 24-25 (1983))*. Maryland law regarding contract interpretation requires the court first to "determine from the language of the agreement itself what a reasonable person in the position of the parties would have meant at the time it was effectuated." *GMAC v. Daniels, 303 Md. 254, 262, 492 A.2d 1306, 1310 (Md. 1985)*. If the language of the contract is clear and unambiguous, then the Court "must presume that the parties meant what they expressed." Id. If the language of the contract is ambiguous, however, the court may consider parole evidence to determine the intent of the parties. E.g. *Truck Ins. Exch. v. Marks Rentals, Inc., 288 Md. 428, 433, 418 A.2d 1187, 1190 (Md. 1980).* Contract language is ambiguous if it could be read to have more than one meaning by a reasonably prudent layperson. *Clendenin Bros., Inc. v. United States Fire Ins. Co., 390 Md. 449, 459, 889 A.2d 387, 393-394 (Md. 2006)*, citing *Truck Ins. Exch., 288 Md. at 433, 418 A.2d at 1190.*

Here, I find that the language of the arbitration agreement is ambiguous; it could be read either to permit the arbitrator to determine the amount of damage to Chessie, or to limit his authority to determining only whether the claimed damages were caused by the lightning strike. Under normal circumstances, the Court would look to the documentary evidence provided by the parties, which in this case includes the arbitration agreement, award, and copies of e-mail correspondence between counsel, ostensibly supplied as extrinsic evidence of the parties' intent with regard to the scope of the arbitration agreement. In this case, however, the admissibility problems with the evidence presented are manifest. First, none of the documentary evidence presented is authenticated by affidavit or otherwise. Next, most of the facts relevant to the contract negotiations at issue have been provided by counsel ipse dixit, without supporting affidavits or deposition testimony. The evidentiary problems associated with the copies of e-mail offered as parol evidence likewise are substantial because they were not authenticated, but instead were simply attached to the parties' motions as exhibits.

Because neither party to this dispute complied with the requirements of *Rule 56* that they support their motions with admissible evidence, I dismissed both motions without prejudice to allow resubmission with proper evidentiary support. (Paper No. 26). I further observed that the unauthenticated e-mails are a form of computer generated evidence that pose evidentiary issues that are highlighted by their electronic medium. 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. Although cases abound regarding the discoverability of electronic records, research has failed to locate a comprehensive analysis of the many interrelated evidentiary issues associated with electronic evidence. Because there is a need for guidance to the bar regarding this subject, this opinion undertakes a broader and more detailed analysis of these issues than would be required simply to resolve the specific issues presented in this case. It is my hope that it will provide a helpful starting place for understanding the challenges associated with the admissibility of electronic evidence.

ADMISSIBILITY OF ELECTRONICALLY STORED INFORMATION

Be careful what you ask for, the saying goes, because you might actually get it. For the last several years there has been seemingly endless discussion of the rules regarding the discovery of electronically stored information ("ESI"). The adoption of a series of amendments to the Federal Rules of Civil Procedure relating to the discovery of ESI in December of 2006 has only heightened, not lessened, this discussion. Very little has been written, however, 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. *FED. R. CIV. P. 56(e)*. This is unfortunate, because considering the significant costs associated with discovery of ESI, it makes little sense to go to all the bother and expense to get electronic information only to have it excluded from evidence or rejected from consideration during summary judgment because the proponent cannot lay a sufficient foundation to get it admitted. The process is complicated by the fact that ESI comes in multiple evidentiary "flavors," including e-mail, website ESI, internet postings, digital photographs, and computer-generated documents and data files.

Whether ESI is admissible into evidence is determined by a collection of evidence rules that present themselves like a series of hurdles to be cleared by the proponent of the evidence. Failure to clear any of these evidentiary hurdles means that the evidence will not be admissible. [Among them is whether] is it authentic as required by *Rule 901(a)* (can the proponent show that the ESI is what it purports to be)?

* * *

Authenticity (*Rules 901-902*)

In order for ESI to be admissible, it also must be shown to be authentic. *Rule 901(a)* defines what this entails: "[t]he 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." As already noted, "[a]uthentication and identification represent a special aspect of relevancy . . . . This requirement of showing authenticity or identity falls into the category of relevancy dependent upon fulfillment of a condition of fact and is governed by the procedure set forth in *Rule 104(b)*." *FED. R. EVID. 901* advisory committee's note. The requirement of authentication and identification also insures that evidence is trustworthy, which is especially important in analyzing hearsay issues. Indeed, these two evidentiary concepts often are considered together when determining the admissibility of exhibits or documents.

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. This is not a particularly high barrier to overcome. For example, in United States v. Safavian, the court analyzed the admissibility of e-mail, noting,

> [t]he question for the court under *Rule 901* is whether the proponent of the evidence has 'offered a foundation from which the jury could reasonably find that the evidence is what the proponent says it is . . . .' The Court need not find that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury ultimately might do so.

435 F. Supp. 2d at 38 (citations omitted)). See also *United States v. Meienberg, 263 F.3d 1177, 1180 (10th Cir. 2001)* (analyzing admissibility of printouts of computerized records); *United States v. Tank, 200 F.3d 627, 630 (9th Cir. 2000)* (analyzing admissibility of exhibits reflecting chat room conversations); *United States v. Reilly, 33 F.3d 1396, 1404 (3d Cir. 1994)*(discussing admissibility of radiotelegrams); *United States v. Howard-Arias, 679 F.2d 363, 366 (4th Cir. 1982)*[**32] (addressing chain of authenticity); *Telewizja Polska USA, Inc. v. Echostar Satellite Corp., 2004 U.S. Dist. LEXIS 20845, 2004 WL 2367740, at *16 (N.D. Ill. Oct. 15, 2004)* (analyzing admissibility of the content of a website).

Ironically, however, counsel often fail to meet even this minimal showing when attempting to introduce ESI, which underscores the need to pay careful attention to this requirement. Indeed, the inability to get evidence admitted because of a failure to authenticate it almost always is a self-inflicted injury which can be avoided by thoughtful advance preparation. See, e.g., In *Re Vee Vinhnee, 336 B.R. 437* (proponent failed properly to authenticate exhibits of electronically stored business records); *United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000)* (proponent failed to authenticate exhibits taken from an organization's website); *St. Luke's Cataract and Laser Institute*

*PA v. Sanderson, 2006 U.S. Dist. LEXIS 28873, 2006 WL 1320242, at *3-4 (M.D. Fla. May 12, 2006)* (excluding exhibits because affidavits used to authenticate exhibits showing content of web pages were factually inaccurate and affiants lacked personal knowledge of facts); *Rambus, Inc. v. Infineon Techs. AG, 348 F. Supp. 2d 698 (E.D. Va. 2004)* (proponent failed to authenticate computer generated business records); *Wady v. Provident Life and Accident Ins. Co. of Am., 216 F. Supp. 2d 1060 (C.D. Cal. 2002)* (sustaining an objection to affidavit of witness offered to authenticate exhibit that contained documents taken from defendant's website because affiant lacked personal knowledge); *Indianapolis Minority Contractors Assoc. Inc. v. Wiley, 1998 U.S. Dist. LEXIS 23349, 1998 WL 1988826, at *7 (S.D. Ind. May 13, 1998)* (proponent of computer records failed to show that they were from a system capable of producing reliable and accurate results, and therefore, failed to authenticate them).

Although courts have recognized that authentication of ESI may require greater scrutiny than that required for the authentication of "hard copy" documents, they have been quick to reject calls to abandon the existing rules of evidence when doing so. For example, in In Re F.P., A Minor the court addressed the authentication required to introduce transcripts of instant message conversations. In rejecting the defendant's challenge to this evidence, it stated:

> Essentially, appellant would have us create a whole new body of law just to deal with e-mails or instant messages. The argument is that e-mails or text messages are inherently unreliable because of their relative anonymity and the fact that while an electronic message can be traced to a particular computer, it can rarely be connected to a specific author with any certainty. Unless the purported author is actually witnessed sending the e-mail, there is always the possibility it is not from whom it claims. As appellant correctly points out, anybody with the right password can gain access to another's e-mail account and send a message ostensibly from that person. However, the same uncertainties exist with traditional written documents. A signature can be forged; a letter can be typed on another's typewriter; distinct letterhead stationary can be copied or stolen. We believe that e-mail messages and similar forms of electronic communication can be properly authenticated within the existing framework of *PaR.E. 901* and Pennsylvania case law . . . We see no justification for constructing unique rules of admissibility of electronic communications such as instant messages; they are to be evaluated on a case-by-case basis as any other document to determine whether or not there has been an adequate foundational showing of their relevance and authenticity. *878 A.2d at 95-96*. Indeed, courts increasingly are demanding that proponents of evidence obtained from electronically stored information pay more attention to the foundational requirements than has been customary for introducing evidence not produced from electronic sources. As one respected commentator on the Federal Rules of Evidence has noted:

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 need for authentication and an explanation of the computer's processing will depend on the complexity and novelty of the computer processing. There are many states in the development of computer data where error can be introduced, which can adversely affect the accuracy and reliability of the output. Inaccurate results occur most often because of bad

or incomplete data inputting, but can also happen when defective software programs are used or stored-data media become corrupted or damaged.

The authentication requirements of *Rule 901* are designed to set up a threshold preliminary standard to test the reliability of evidence, subject to later review by an opponent's cross-examination. 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.

> Determining what degree of foundation is appropriate in any given case is in the judgment of the court. The required foundation will vary not only with the particular circumstances but also with the individual judge.

WEINSTEIN at § 900.06[3]. Obviously, there is no "one size fits all" approach that can be taken when authenticating electronic evidence, in part because technology changes so rapidly that it is often new to many judges.

Although *Rule 901(a)* addresses the requirement to authenticate electronically generated or electronically stored evidence, it is silent regarding how to do so. *Rule 901(b)*, however, provides examples of how authentication may be accomplished. It states:

> (b) Illustrations. By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule:
> (1) Testimony of witness with knowledge. Testimony that a matter is what it is claimed to be.
> * * *
> (3) Comparison by trier or expert witness. Comparison by the trier of fact or by expert witnesses with specimens which have been authenticated.
> (4) Distinctive characteristics and the like. Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances.
>
> * * *
> (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.
> * * *
> (9) Process or system. Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.
> * * *

The ten methods identified by *Rule 901(b)* are non-exclusive. *FED. R. EVID. 901(b)* advisory committee's note ("The examples are not intended as an exclusive enumeration of allowable methods but are meant to guide and suggest, leaving room for growth and development in this area of the law."); WEINSTEIN at § 901.03[1] ("Parties may use any of the methods listed in *Rule 901(b)*, any combination of them, or any other proof that may be available to carry their burden of showing that the proffered exhibit is what they claim it to be."); *Telewizja Polska USA, 2004 U.S. Dist. LEXIS 20845, 2004 WL 2367740* (authentication methods listed in *Rule 901(b)* are "non-exhaustive"). See also *United States v. Simpson, 152 F.3d 1241, 1249 (10th Cir. 1998)* (evaluating methods of authenticating a printout of the text of a chat room discussion between the defendant and an undercover detective in a child pornography case).

Although the methods of authentication listed in *Rule 901(b)* "relate for the most part to documents . . . some attention [has been] given to . . . computer print-outs," particularly *Rule 901(b)(9)*, which was drafted with "recent developments" in computer technology in mind. *FED. R. EVID. 901(b)* advisory committee's note. When faced with resolving authentication issues for electronic evidence, courts have used a number of the methods discussed in *Rule 901(b)*, as well as approved some methods not included in that rule:

> This rule permits authentication by: "[t]estimony that a matter is what it is claimed to be." This rule "contemplates a broad spectrum" including "testimony of a witness who was present at the signing of a document . . . ." *FED. R. EVID. 901(a)* advisory committee's note. "[1]n recognition of the proponent's light burden of proof in authenticating an exhibit . . . the 'knowledge' requirement of *Rule 901(b)(1)* is liberally construed. A witness may be appropriately knowledgeable through having participated in or observed the event reflected by the exhibit." WEINSTEIN at § 901.03[2] (cross-reference omitted). Courts considering the admissibility of electronic evidence frequently have acknowledged that it may be authenticated by a witness with personal knowledge. *United States v. Kassimu, 188 Fed. Appx. 264, 2006 WL 1880335 (5th Cir. 2006)* (ruling that copies of a post office's computer records could be authenticated by a custodian or other qualified witness with personal knowledge of the procedure that generated the records); *St. Luke's, 2006 U.S. Dist. LEXIS 28873, 2006 WL 1320242 at *3-4* ("To authenticate printouts from a website, the party proffering the evidence must produce 'some statement or affidavit from someone with knowledge [of the website] . . . for example [a] web master or someone else with personal knowledge would be sufficient.'" (citation omitted)); *Safavian, 435 F. Supp. 2d at 40 n.2 (D.D.C. 2006)* (noting that e-mail may be authenticated by a witness with knowledge that the exhibit is what it is claimed to be); *Wady, 216 F. Supp 2d 1060* (sustaining objection to affidavit[**42] of plaintiff's witness attempting to authenticate documents taken from the defendant's website because the affiant lacked personal knowledge of who maintained the website or authored the documents). 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. WEINSTEIN at § 901.03[2]. n22 It is necessary, however, that the authenticating witness 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, 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)*.

Rule 901(b)(3).

This rule allows authentication or identification by "[c]omparison by the trier of fact or by expert witnesses with specimens which have been authenticated." Interestingly, the rule allows either expert opinion testimony to authenticate a questioned document by comparing it to one known to be authentic, or by permitting the factfinder to do so. Obviously, the specimen used for the comparison with the document to be authenticated must be shown itself to be authentic. WEINSTEIN at § 901.03[7][b]. This may be accomplished by any means allowable by *Rule 901* or *902*, as well as by using other exhibits already admitted into evidence at trial, or admitted into evidence by judicial notice under *Rule 201*. Id. Although the common law origin of *Rule 901(b)(3)* involved its use for authenticating handwriting or signatures, *FED. R. EVID. 901(b)(3)* advisory committee's note, it now is commonly used to authenticate documents, WEINSTEIN at § 901.03[7][b], and at least one court has noted its appropriate use for authenticating e-mail. *Safavian, 435 F. Supp. 2d at 40* (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)*.").

Rule 901(b)(4).

This rule is one of the most frequently used to authenticate e-mail and other electronic records. It permits exhibits to be authenticated or identified by "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." The commentary to *Rule 901(b)(4)* observes [t]he characteristics of the offered item itself, considered in the light of circumstances, afford authentication techniques in great variety," including 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. *FED. R. EVID. 901(b)(4)* advisory committee's note. Use of this rule often is characterized as authentication solely by "circumstantial evidence." WEINSTEIN at § 901.03[8]. Courts have recognized this rule as a means to authenticate ESI, including e-mail, text messages and the content of websites. See *United States v. Siddiqui, 235 F.3d 1318, 1322-23 (11th Cir. 2000)* (allowing the authentication of an e-mail entirely by circumstantial evidence, including the presence of the defendant's work e-mail address, content of which the defendant was familiar with, use of the defendant's nickname, and testimony by witnesses that the defendant spoke to them about the subjects contained in the e-mail); *Safavian, 435 F. Supp. 2d at 40* (same result regarding e-mail); In *Re F.P., a Minor, 878 A.2d at 94* (noting that authentication could be accomplished by direct evidence, circumstantial evidence, or both, but ultimately holding that transcripts of instant messaging conversation circumstantially were authenticated based on presence of defendant's screen name, use of defendant's first name, and content of threatening message, which other witnesses had corroborated); *Perfect 10, Inc. v.*

Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1153-54 (C.D. Cal. 2002) (admitting website postings as evidence due to circumstantial indicia of authenticity, including dates and presence of identifying web addresses).

One method of authenticating electronic evidence under *Rule 901(b)(4)* is the use of "hash values" or "hash marks" when making documents. A hash value is:

> 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.

Federal Judicial Center, Managing Discovery of Electronic Information: A Pocket Guide for Judges, Federal Judicial Center, 2007 at 24. 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. This underscores a point that counsel often overlook. A party that seeks to introduce its own electronic records may have just as much difficulty authenticating them as one that attempts to introduce the electronic records of an adversary. Because it is so common for multiple versions of electronic documents to exist, it sometimes is difficult to establish that the version that is offered into evidence is the "final" or legally operative version. This can plague a party seeking to introduce a favorable version of its own electronic records, when the adverse party objects that it is not the legally operative version, given the production in discovery of multiple versions. 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)*.

Another way in which electronic evidence may be authenticated under *Rule 901(b)(4)* is by examining the metadata for the evidence. Metadata, commonly described as "data about data," is defined as "information describing the history, tracking, or management of an electronic document." Appendix F to The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age defines metadata 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)." Technical Appendix E to the Sedona Guidelines provides an extended description of metadata. It further defines metadata to include "all of the contextual, processing, and use information needed to identify and certify the scope, authenticity, and integrity of active or archival electronic information or records." Some examples of metadata for electronic documents include: a file's name, a file's location (e.g., directory structure or pathname), file format or file type, file size, file dates (e.g., creation date, date of last data modification, date of last data access, and date of last metadata modification), and file permissions (e.g., who can read the data, who can write to it, who can run it). Some metadata, such as file dates and sizes, can easily be seen by users; other

metadata can be hidden or embedded and unavailable to computer users who are not technically adept. *Williams v. Sprint/United Mgmt. Co., 230 F.R.D. at 646* (footnote omitted); Federal Judicial Center, Managing Discovery of Electronic Information: A Pocket Guide for Judges, Federal Judicial Center, 2007 at 24-25 (defining metadata as "[i]nformation about a particular data set or document which describes how, when, and by whom the data set or document was collected, created, accessed, or modified . . . "). Recently revised *Federal Rule of Civil Procedure 34* permits a party to discover electronically stored information and to identify the form or forms in which it is to be produced. A party therefore can request production of electronically stored information in its "native format", which includes the metadata for the electronic document. n25 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)*. Although specific source code markers that constitute metadata can provide a useful method of authenticating electronically stored evidence, this method is not foolproof because,

> [a]n unauthorized person may be able to obtain access to an unattended computer. Moreover, a document or database located on a networked-computer system can be viewed by persons on the network who may modify it. In addition, many network computer systems usually provide for a selected network administrators to override an individual password identification number to gain access when necessary.

WEINSTEIN at § 900.01[4][a]; see also *Fennell v. First Step Designs, Ltd., 83 F.3d 526, 530 (1st Cir. 1996)* (discussing how metadata markers can reflect that a document was modified when in fact it simply was saved to a different location). Despite its lack of conclusiveness, however, metadata certainly is a useful tool for authenticating electronic records by use of distinctive characteristics.

Rule 901(b)(7):

This Rule permits authentication by:

> 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.

The commentary to *Rule 901(b)(7)* recognizes that it applies to computerized public records, noting that "[p]ublic records are regularly authenticated by proof of custody, without more. [*Rule 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." *FED. R. EVID. 901(b)(7)* advisory committee's note (citation omitted). 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." WEINSTEIN at § 901.10[2]. This may be done by "[a] certificate of authenticity from the public office; [t]he testimony of an officer who is authorized to attest to custodianship, [or] the testimony of a witness with knowledge that the evidence is in fact from a public office authorized to keep such a record." Id. (footnote omitted). 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. Id.

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. For example, in United States v. Meienberg, the court rejected defendant's challenge to the admissibility of a law enforcement agency's computerized records. Defendant argued that the only way they could be authenticated was under *Rule 901(b)(9)*, through proof that they were produced by a system or process capable of producing a reliable result. Defendant further argued that the records had not been shown to be accurate. The appellate court disagreed, holding that the records properly had been authenticated under *Rule 901(b)(7)*, which did not require a showing of accuracy. The court noted that any question regarding the accuracy of the records went to weight rather than admissibility. *263 F.3d at 1181*. Thus, a decision to authenticate under *Rule 901(b)(7)*, as opposed to *901(b)(9)* may mean that the required foundation is much easier to prove. This underscores the importance of the point previously made, that there may be multiple ways to authenticate a particular computerized record, and careful attention to all the possibilities may reveal a method that significantly eases the burden of authentication.

Rule 901(b)(9):

This Rule recognizes one method of authentication that is particularly useful in authenticating electronic evidence stored in or generated by computers. It authorizes authentication by "[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result." *FED. R. EVID. 901(b)(9)*. This rule was "designed for situations in which the accuracy of a result is dependent upon a process or system which produces it." *FED. R. EVID. 901(b)(9)* advisory committee's note. See also WEINSTEIN at § 901.12[3]; n26 In *Re Vee Vinhnee, 336 B.R. at 446* ("*Rule 901(b)(9)*, which is designated as an example of a satisfactory authentication, describes the appropriate authentication for results of a process or system and contemplates evidence describing the process or system used to achieve a result and demonstration that the result is accurate. The advisory committee note makes plain that *Rule 901(b)(9)* was designed to encompass computer-generated evidence. . .").

Rule 902:

In addition to the non-exclusive methods of authentication identified in *Rule 901(b)*, *Rule 902* identifies twelve methods by which documents, including electronic ones, may be authenticated without extrinsic evidence. This is commonly referred to as "self-authentication." The rule states:

> Extrinsic evidence of authenticity as a condition precedent to admissibility is not required with respect to the following:
> * * *
> (5) Official publications. Books, pamphlets, or other publications purporting to be issued by public authority.
> * * *

(7) Trade inscriptions and the like. Inscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin.

* * *

(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:

(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.

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. Because *Rule 104(b)* applies in such cases, the exhibit and the evidence challenging its authenticity goes to the jury, which ultimately determines whether it is authentic. *FED. R. EVID. 902* advisory committee's note. Some of the examples contained in *Rule 902*, such as *Rule 902(3)* (foreign public documents), *902(4)* (certified copies of public records), *902(8)* (acknowledged documents), *902(11)* (certified copies of domestic records of a regularly conducted activity), and *902(12)* (certified foreign records of regularly conducted activity), do require a[**63] certificate signed by a custodian or other qualified person to accomplish the self-authentication.

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). The first, *Rule 902(5)*, provides:

(5) Official publications. Books, pamphlets, or other publications purporting to be issued by public authority.

The rule "[dispenses] with preliminary proof of the genuineness of purportedly official publications . . . . [but] does not confer admissibility upon all official publications; it merely provides a means whereby their authenticity may be taken as established for purposes of admissibility." *FED. R. EVID. 902(5)* advisory committee's note. This means that, to be admissible, the proponent may also

need to establish that the official record qualifies as a public record hearsay exception under *Rule 803(8)*. WEINSTEIN at § 902.02[2]. Although the rule is silent regarding the[**64] level of government that must authorize the publication, commentators suggest that the list includes the United States, any State, district, commonwealth, territory or insular possession of the United States, the Panama Canal Zone, the Trust Territory of the Pacific islands, or a political subdivision, department, officer, or agency of any of the foregoing. Id.

In Equal Employment Opportunity Commission v. E. I. DuPont De Nemours and Co., the court admitted into evidence printouts of postings on the website of the United States Census Bureau as self-authenticating under *Rule 902(5)*. *2004 U.S. Dist. LEXIS 20748, 2004 WL 2347556 (E.D. La. Oct. 18, 2004)*. 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.

Rule 902(7) provides that exhibits may be self-authenticated by "[i]nscriptions, signs, tags, or[**65] labels purporting to have been affixed in the course of business and indicating ownership, control, or origin." 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 [*552] employer-company. The identification marker alone may be sufficient to authenticate an e-mail under *Rule 902(7)*." WEINSTEIN at § 900.07[3][c].

Rule 902(11) also is extremely useful because it affords a means of authenticating business records under *Rule 803(6)*, one of the most used hearsay exceptions, without the need for a witness to testify in person at trial. It 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:
>
> (A) was made at or near the time of the[**66] 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.

This rule was added in the 2000 amendments to the Federal Rules of Evidence, and it was intended to "[set] forth a procedure by which parties can authenticate certain records of regularly conducted

activity, other than through the testimony of a foundation witness." *FED. R. EVID. 902(11)* advisory committee's note. Unlike most of the other authentication rules, *Rule 902(11)* also contains a notice provision, requiring the proponent to provide written notice of the intention to use the rule to all adverse parties and to make available to them the records[**67] sufficiently in advance of litigation to permit a fair opportunity to challenge them. WEINSTEIN at § 902.13[2]. Because compliance with *Rule 902(11)* requires the proponent to establish all the elements of the business record exception to the hearsay rule, *Rule 803(6)*, courts usually analyze the authenticity issue under *Rule 902(11)* concomitantly with the business record hearsay exception. n28 *Rambus, 348 F. Supp. 2d at 701* ("Thus, the most appropriate way to view *Rule 902(11)* is as the functional equivalent of testimony offered to authenticate a business record tendered under *Rule 803(6)* because the declaration permitted by *Rule 902(11)* serves the same purpose as authenticating testimony . . . [B]ecause *Rule 902[11]* contains the same requirements, and almost the same wording, as *Rule 803(6)*, decisions explaining the parallel provisions of *Rule 803(6)* are helpful in resolving the issues here presented."); In *Re Vee Vinhnee, 336 B.R. at 444* (stating that in deciding whether to admit business records, the authenticity analysis is merged into the business record analysis).

Finally, as noted at the beginning of this discussion regarding the authenticating electronic records, *Rule 901(b)* makes clear that the ten examples listed are illustrative only, not exhaustive. In ruling on whether electronic evidence has been properly authenticated, courts have been willing to think "outside of the box" to recognize new ways of authentication. For example, they 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. *Indianapolis Minority Contractors Ass'n., 1998 U.S. Dist. LEXIS 23349, 1998 WL 1988826, at *6* ("The act of production is an implicit authentication of documents produced . . . . *Federal Rule of Evidence 901* provides that '[t]he 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. Defendants admit that they did produce [the exhibits at issue]. . . . Thus . . . the 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." (citation omitted)); Perfect 10, *213 F. Supp. 2d at 1153-54* (finding that exhibits of website postings had been properly authenticated for three reasons, including that certain of them had been provided to the plaintiff by the defendant during discovery).

In Telewizja Polska USA, the court embraced a non-traditional method of authentication when faced with determining whether exhibits depicting the content of the defendant's website at various dates several years in the past were admissible. *2004 U.S. Dist. LEXIS 20845, 2004 WL 2367740*. The plaintiff offered 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 though use of its "wayback machine." n29 The defendant objected, contending that the Internet Archive was not a reliable source, and thus the exhibits had not been authenticated. The court disagreed, stating:

> *Federal Rule of Evidence 901* 'requires only a prima facie showing of genuineness and leaves it to the jury to decide the true authenticity and probative value of the evidence.' Admittedly, the Internet Archive does not fit neatly into any of the non-exhaustive examples listed in *Rule 901*; the Internet Archive is a relatively new

> source for archiving websites. Nevertheless, Plaintiff has presented no evidence that the Internet Archive is unreliable or biased. And Plaintiff has neither denied that the exhibit represents the contents of its website on the dates in question, nor come forward with its own evidence challenging the veracity of the exhibit. Under these circumstances, the Court is of the opinion that [the affidavit from the representative of the Internet Archive Company] is sufficient to satisfy *Rule 901*'s threshold requirement for admissibility.

*Id. at *6*.

[**71] Additionally, authentication may be accomplished by the court taking judicial notice under *Rule 201* of certain foundational facts needed to authenticate an electronic record. Under this rule, the parties may request the court to take judicial notice of adjudicative facts that are 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. *FED. R. EVID. 201 (b)*; WEINSTEIN at § 201.12[1]. Judicial notice could be a helpful way to establish certain well known characteristics of computers, how the internet works, scientific principles underlying calculations performed within computer programs, and many similar facts that could facilitate authenticating electronic evidence.

Authentication also can be accomplished in civil cases by taking advantage of *FED. R. CIV. P. 36*, which permits a party to request that his or her opponent admit the "genuineness of documents." Also, at a pretrial conference, pursuant to *FED. R. CIV. P. 16(c)(3)*[**72] , a party may request that an opposing party agree to stipulate "regarding the authenticity of documents," and the court may take "appropriate action" regarding that request. Similarly, if 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 good cause. This means that if the opposing party does not raise authenticity objections within the fourteen days, they are waived.

The above discussion underscores the need for counsel to be creative in identifying methods of authenticating electronic evidence when the facts support a conclusion that the evidence is reliable, accurate, and authentic, regardless of whether there is a particular example in *Rules 901* and *902* that neatly fits.

Finally, any serious consideration of the requirement to authenticate electronic evidence needs to acknowledge that, given the [*554] wide diversity of such evidence, there is no single approach to authentication that will work in all instances. [**73] It is possible, however, to identify certain authentication issues that have been noted by courts and commentators with particular types of electronic evidence and to be forearmed with this knowledge to develop authenticating facts that address these concerns.

E-mail

There is no form of ESI more ubiquitous than e-mail, and it is the category of ESI at issue in this case. Although courts today have more or less resigned themselves to the fact that "[w]e live in an

age of technology and computer use where e-mail communication now is a normal and frequent fact for the majority of this nation's population, and is of particular importance in the professional world," *Safavian, 435 F. Supp. 2d at 41*, it was not very long ago that they took a contrary view -- "[e]-mail is far less of a systematic business activity than a monthly inventory printout." *Monotype Corp. PLC v. Int'l Typeface, 43 F.3d 443, 450 (9th Cir. 2004)* (affirming trial court's exclusion of e-mail as inadmissible as a business record). 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[**74] 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. Indeed, it is not unusual to see a case consisting almost entirely of e-mail evidence. See, e.g., *Safavian, 435 F. Supp. 2d 36*.

Not surprisingly, there are many ways in which e-mail evidence may be authenticated. One well respected commentator has observed:

> [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.

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[**75] 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.

WEINSTEIN at § 900.07[3][c]; see also EDWARD J. IMWINKELRIED, EVIDENTIARY FOUNDATIONS § 4.03 [4][b] (LexisNexis 6th ed. 2005)(hereinafter[**76] "IMWINKELRIED, EVIDENTIARY FOUNDATIONS.") Courts also have approved the authentication of e-mail by the above described methods. See, e.g., *Siddiqui, 235 F.3d at 1322-23* (E-mail may be authenticated entirely by circumstantial evidence, including its distinctive characteristics); *Safavian, 435 F. Supp.*

2d at 40 (recognizing that e-mail may be authenticated by distinctive characteristics (*901(b)(4)*, or by comparison of exemplars with other e-mails that already have been authenticated (*901(b)(3)*); *Rambus, 348 F. Supp. 2d 698* (E-mail that qualifies as business record may be [*555] self-authenticating under *902(11)*); In *Re F.P., A Minor, 878 A.2d at 94* (E-mail may be authenticated by direct or circumstantial evidence).

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).

Internet Website Postings

Courts often have been faced with determining the admissibility of exhibits containing representations of the contents of website postings of a party at some point relevant to the litigation. Their reaction has ranged from the famous skepticism expressed in *St.Clair v. Johnny's Oyster and Shrimp, Inc. 76 F. Supp. 2d 773 (S.D. Tex. 1999)*, n30 to more permissive approach taken in *Perfect 10, 213 F. Supp. 2d at 1153-54*.

The issues that have concerned courts include the possibility that third persons other than the sponsor of the website were responsible for the content of the postings, leading many to require proof by the proponent that the organization hosting the website actually posted the statements or authorized their posting. See *United States v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000)* (excluding evidence of website postings because proponent failed to show [**79]that sponsoring organization actually posted the statements, as opposed to a third party); *St. Luke's, 2006 U.S. Dist. LEXIS 28873, 2006 WL 1320242* (plaintiff failed to authenticate exhibits of defendant's website postings because affidavits used to authenticate the exhibits were factually inaccurate and the author lacked personal knowledge of the website); *Wady, 216 F. Supp. 2d 1060*. One commentator has observed "[i]n 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?" n32 The same author suggests that the following factors will influence courts in ruling whether to admit evidence of internet postings:

> The length of time the data was posted on the site; whether others report having seen it; whether it remains on the website for the court to verify; whether the data is of a type ordinarily posted on that website or websites of similar entities (e.g. financial information from corporations); whether the owner of the site has elsewhere published[**80] the same data, in whole or in part; whether others have published the same data, in whole or in part; whether the data [*556] has been republished by others who identify the source of the data as the website in question? n33

Counsel attempting to authenticate exhibits containing information from internet websites need to address these concerns in deciding what method of authentication to use, and the facts to include in the foundation. 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).

Text Messages and Chat Room Content

Many of the same foundational issues found encountered when authenticating website evidence apply with equal force to text messages[**81] and internet chat room content; however, the fact that chat room messages are posted by third parties, often using "screen names" means that it cannot be assumed that the content found in chat rooms was posted with the knowledge or authority of the website host. SALTZBURG at § 901.02[12]. One commentator has suggested that the following foundational requirements must be met to authenticate chat room evidence:

> (1) [e]vidence that the individual used the screen name in question when participating in chat room conversations (either generally or at the site in question); (2) [e]vidence that, when a meeting with the person using the screen name was arranged, the individual . . . showed up; (3) [e]vidence that the person using the screen name identified [himself] as the [person in the chat room conversation]; evidence that the individual had in [his] possession information given to the person using the screen name; (5) [and] [e]vidence from the hard drive of the individual's computer [showing use of the same screen name].

Id. at § 901.02[12]. Courts also have recognized that exhibits of chat room conversations may be authenticated circumstantially. [**82] For example, in In Re F.P., A Minor, the defendant argued that the testimony of the internet service provider was required, or that of a forensic expert. *878 A.2d at 93-94*. The court held that circumstantial evidence, such as the use of the defendant's screen name in the text message, the use of the defendant's first name, and the subject matter of the messages all could authenticate the transcripts. Id. Similarly, in United States v. Simpson, the court held that there was ample circumstantial evidence to authenticate printouts of the content of chat room discussions between the defendant and an undercover detective, including use of the e-mail name of the defendant, the presence of the defendant's correct address in the messages, and notes seized at the defendant's home containing the address, e-mail address and telephone number given by the undercover officer. *152 F.3d at 1249*. Likewise, in United States v. Tank, the court found sufficient circumstantial facts, to authenticate chat room conversations, despite the fact that certain portions of the text of the messages in which the defendant had participated had been deleted. *200 F.3d at 629-31*.[**83] There, the court found the testimony regarding the limited nature of the deletions by the member of the chat room club who had made the deletions, circumstantial evidence connecting the defendant to the chat room, including the use of the defendant's screen name in the messages, were sufficient to authenticate the messages. *Id. at 631*. Based on the foregoing cases, the 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).

Computer Stored Records and Data

> Given the widespread use of computers, there is an almost limitless variety of records that are stored in or generated by computers. As one commentator has

> observed "[m]any kinds of computer records and computer-generated information are introduced as real evidence or used as litigation aids at trials. They range from computer printouts [*557] of stored digital data to complex computer-generated models performing complicated computations. Each may raise different admissibility issues concerning authentication and other foundational requirements. [**84] " WEINSTEIN at § 900.06[3]. The least complex admissibility issues are associated with electronically stored records. "In general, electronic documents or records that are merely stored in a computer raise no computer-specific authentication issues." WEINSTEIN at § 900.06[3]. That said, although 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. MANUAL FOR COMPLEX LITIGATION at § 11.447; n34 see also IMWINKELRIED, EVIDENTIARY FOUNDATIONS at 4.03[2]. n35

Two cases illustrate the contrast between the more lenient approach to admissibility of computer records and the more demanding one. In United States v. Meienberg, the defendant challenged on appeal the admission into evidence of printouts of computerized records[**86] of the Colorado Bureau of Investigation, arguing that they had not been authenticated because the government had failed to introduce any evidence to demonstrate the accuracy of the records. *263 F.3d at 1180-81*. The Tenth Circuit disagreed, stating:

> Any question as to the accuracy of the printouts, whether resulting from incorrect data entry or the operation of the computer program, as with inaccuracies in any other type of business records, would have affected only the weight of the printouts, not their admissibility.

Id. at 1181 (citation omitted). See also *Kassimu, 188 Fed. Appx. 264, 2006 WL 1880335* (To authenticate computer records as business records did not require the maker, or even a custodian of the record, only a witness qualified to explain the record keeping system of the organization to confirm that the requirements of *Rule 803(6)* had been met, and the inability of a witness to attest to the accuracy of the information entered into the computer did not preclude admissibility); *Sea Land v. Lozen Int'l, 285 F.3d 808 (9th Cir. 2002)* (ruling that trial court properly considered electronically generated bill of lading[**87] as an exhibit to a summary judgment motion. The only foundation that was required was that the record was produced from the same electronic information that was generated contemporaneously when the parties entered into their contact. The court did not require evidence that the records were reliable or accurate).

In contrast, in the case of In Re Vee Vinhnee, the bankruptcy appellate panel upheld the trial ruling of a bankruptcy judge excluding electronic business records of the credit card issuer of a Chapter 7 debtor, for failing to authenticate them. *336 B.R. 437*. The court noted that "it is becoming recognized that early versions of computer foundations were too cursory, even though the basic elements covered the ground." *Id. at 445-46*. The court further observed that:

> The primary authenticity issue in the context of business records is on what has, or may have, happened to the record in the interval between when it was placed in the files and the time of trial. In other words, the record being proffered must be shown

> to continue to be an accurate representation of the record that originally was created . . . . Hence, the focus is not on [**88]the circumstances of the creation of the record, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created. *Id. at 444*. The court reasoned that, for paperless electronic records:

The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. How changes in the database are logged or recorded, as well as the structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database, are pertinent to the question of whether records have been changed since their creation. *Id. at 445*. In order to meet the heightened demands for authenticating electronic business records, the court adopted, with some modification, an eleven-step foundation proposed by Professor Edward Imwinkelried:

Professor Imwinkelried perceives electronic records as a form of scientific evidence and discerns an eleven-step foundation for computer records:

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.

IMWINKELRIED, EVIDENTIARY FOUNDATIONS at § 4.03[2].

As the foregoing cases illustrate, there is a wide disparity between the most lenient positions courts have taken in accepting electronic records as authentic and the most demanding requirements[**91] that have been imposed. Further, it would not be surprising to find that, to date, more courts have tended towards the lenient rather than the demanding approach. However, it also is plain that commentators and courts increasingly recognize the special characteristics of electronically stored records, and there appears to be a growing awareness, as expressed in the Manual for Complex Litigation, n38 that courts "should . . . consider the accuracy and reliability of computerized evidence" in ruling on [*559] its admissibility. Lawyers can expect to encounter judges in both camps, and in the absence of controlling precedent in the court where an action is pending setting forth the foundational requirements for computer records, there is uncertainty about which approach will be required. Further, although " it may be better to be lucky than good," as the saying goes, counsel would be wise not to test their luck unnecessarily. 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. If less is required, then luck was with you.

[**92] 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).

Computer Animation and Computer Simulations.

Two similar, although distinct, forms of computer generated evidence also raise unique authentication issues. The first is computer animation, "the display of a sequence of computer-generated images." IMWINKELRIED, EVIDENTIARY FOUNDATIONS at § 4.09[4][a]. The attraction of this form of evidence is irresistible, because:

> when there is no movie or video of the event being litigated, a computer animation is a superior method of communicating the relevant information to the trier of fact. Absent a movie or video, the proponent might have to rely on static charts or oral testimony to convey a large amount of complex information to the trier of fact. When the proponent relies solely on oral expert testimony, the details may be presented one at a time; but an animation can piece all the details together for the jury. A computer animation in effect[**93] condenses the information into a single evidentiary package. In part due to television, the typical American is a primarily visual learner; and for that reason, in the short term, many jurors find the animation more understandable than charts or oral testimony. Use of an animation can also significantly increase long-term juror retention of the information. Id. at § 4.09[4][a]. The second form of computer generated evidence is a computer simulation. The distinction between them has been explained usefully as follows:

Computer generated evidence is an increasingly common form of demonstrative evidence. If the purpose of the computer evidence is to illustrate and explain a witness's testimony, courts usually refer to the evidence as an animation. In contrast, a simulation is based on scientific or physical principles and data entered into a computer, which is programmed to analyze the data and draw a conclusion from it, and courts generally require proof to show the validity of the science before the simulation evidence is admitted

> Thus, the classification of a computer-generated exhibit as a simulation or an animation also affects the evidentiary foundation[**94] required for its admission.

State v. Sayles, 662 N.W.2d 1, 9 (Iowa 2003) (citation omitted).

Courts generally have allowed the admission of computer animations if authenticated by testimony of a witness with personal knowledge of the content of the animation, upon a showing that it fairly and adequately portrays the facts and that it will help to illustrate the testimony given in the case. This usually is the sponsoring witness. *Id. at 10* (state's expert witness had knowledge of content of shaken infant syndrome animation and could testify that it correctly and adequately portrayed the facts that would illustrate her testimony); *Hinkle v. City of Clarksburg, 81 F.3d 416 (4th Cir. 1996)* (holding that a computer-animated videotaped recreation of events at issue in trial is not unduly prejudicial if it is sufficiently close to the actual events and is not confused by the jury for the real life events themselves); *Friend v. Time Mfg. Co., 2006 U.S. Dist. LEXIS 52790, 2006 WL 2135807, at *7 (D. Ariz. July 28, 2006)* ("The use of computer animations is allowed when it satisfies the usual foundational requirements for demonstrative evidence. [**95] 'At a minimum, the animation's proponent must show the computer simulation fairly and accurately depicts [*560] what it represents, whether through the computer expert who prepared it or some other witness who is qualified to so testify, and the opposing party must be afforded an opportunity for cross-examination." (citation omitted)); *People v. Cauley, 32 P.3d 602 (Colo. 2001)* (holding that, "[a] computer animation is admissible as demonstrative evidence if the proponent of the video proves that it: 1) is authentic . . .; 2) is relevant . . .; 3) is a fair and accurate representation of the evidence to which it relates; and 4) has a probative value that is not substantially outweighed by the danger of unfair prejudice . . ."); *Clark v. Cantrell, 339 S.C. 369, 529 S.E.2d 528 (S.C. 2000)* ("[A] party may authenticate a video animation by offering testimony from a witness familiar with the preparation of the animation and the data on which it is based . . . [including] the testimony of the expert who prepared the underlying data and the computer technician who used that data to create it." (citation omitted)). Thus, the most frequent methods of authenticating computer [**96]animations are *901(b)(1)* (witness with personal knowledge), and *901(b)(3)* (testimony of an expert witness).

Computer simulations are treated as a form of scientific evidence, offered for a substantive, rather than demonstrative purpose. WEINSTEIN at § 900,03[1] (p. 900-21); IMWINKELRIED, EVIDENTIARY FOUNDATIONS at § 4.09[4][a],[c]. The case most often cited with regard to the foundational requirements needed to authenticate a computer simulation is Commercial Union v. Boston Edison, where the court stated:

> The function of computer programs like TRACE 'is to perform rapidly and accurately an extensive series of computations not readily accomplished without use of a computer.' We permit experts to base their testimony on calculations performed by hand. There is no reason to prevent them from performing the same calculations, with far greater rapidity and accuracy, on a computer. Therefore . . . we treat computer-generated models or simulations like other scientific tests, and condition admissibility on a sufficient showing that: (1) the computer is functioning properly; (2) the input and underlying equations are sufficiently complete and accurate (and

> disclosed[**97] to the opposing party, so that they may challenge them); and (3) the program is generally accepted by the appropriate community of scientists.

412 Mass. 545, 591 N.E.2d 165, 168 (Mass. 1992) (citation omitted). The Commercial Union test has been followed by numerous courts in determining the foundation needed to authenticate computer simulations. For example, in State v. Swinton, the court cited with approval Commercial Union, but added that the key to authenticating computer simulations is to determine their reliability. *268 Conn. 781, 847 A.2d 921, 942 (Conn. 2004)*. In that regard, the court noted that the following problems could arise with this type of computer evidence: (1) the underlying information itself could be unreliable; (2) the entry of the information into the computer could be erroneous; (3) the computer hardware could be unreliable; (4) the computer software programs could be unreliable; (5) "the execution of the instructions, which transforms the information in some way--for example, by calculating numbers, sorting names, or storing information and retrieving it later" could be unreliable; (6) the output of the computer--the printout, transcript, or[**98] graphics, could be flawed; (7) the security system used to control access to the computer could be compromised; and (8) the user of the system could make errors. The court noted that *Rule 901(b)(9)* was a helpful starting point to address authentication of computer simulations. Id.; see also *Bray v. Bi-State Dev. Corp., 949 S.W.2d 93 (Mo. Ct. App. 1997)* (citing Commercial Union and ruling that authentication properly was accomplished by a witness with knowledge of how the computer program worked, its software, the data used in the calculations, and who verified the accuracy of the calculations made by the computer with manual calculations); *Kudlacek v. Fiat, 244 Neb. 822, 509 N.W.2d 603, (Neb. 1994)* (citing Commercial Union and holding that computer simulation was authenticated by the plaintiff's expert witness). Thus, the 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 [*561] involve *Federal Rules of Evidence 702* and *703*[**99] .

Digital Photographs

Photographs have been authenticated for decades under *Rule 901(b)(1)* by the testimony of a witness familiar with the scene depicted in the photograph who testifies that the photograph fairly and accurately represents the scene. Calling the photographer or offering exert testimony about how a camera works almost never has been required for traditional film photographs. Today, however, the vast majority of photographs taken, and offered as exhibits at trial, are digital photographs, which are not made from film, but rather from images captured by a digital camera and loaded into a computer. Digital photographs present unique authentication problems because they are a form of electronically produced evidence that may be manipulated and altered. Indeed, unlike photographs made from film, digital photographs may be "enhanced." Digital image "enhancement consists of removing, inserting, or highlighting an aspect of the photograph that the technician wants to change." Edward J. Imwinkelried, Can this Photo be Trusted?, Trial, October 2005, at 48. Some examples graphically illustrate the authentication issues associated with digital enhancement of photographs:[**100]

> [S]uppose that in a civil case, a shadow on a 35 mm photograph obscures the name of the manufacturer of an offending product. The plaintiff might offer an enhanced image, magically stripping the shadow to reveal the defendant's name. Or suppose

> that a critical issue is the visibility of a highway hazard. A civil defendant might offer an enhanced image of the stretch of highway to persuade the jury that the plaintiff should have perceived the danger ahead before reaching it. In many criminal trials, the prosecutor offers an 'improved', digitally enhanced image of fingerprints discovered at the crime scene. The digital image reveals incriminating points of similarity that the jury otherwise would never would have seen.

Id. at 49. There are three distinct types of digital photographs that should be considered with respect to authentication analysis: original digital images, digitally converted images, and digitally enhanced images. Id.

An original digital photograph may be authenticated the same way as a film photo, by a witness with personal knowledge of the scene depicted who can testify that the photo fairly and accurately depicts it. Id. If a question [**101]is raised about the reliability of digital photography in general, the court likely could take judicial notice of it under *Rule 201*. Id. For digitally converted images, authentication requires an explanation of the process by which a film photograph was converted to digital format. This would require testimony about the process used to do the conversion, requiring a witness with personal knowledge that the conversion process produces accurate and reliable images, *Rules 901(b)(1)* and *901(b)(9)*-the later rule implicating expert testimony under *Rule 702*. Id. Alternatively, if there is a witness familiar with the scene depicted who can testify that the photo produced from the film when it was digitally converted, no testimony would be needed regarding the process of digital conversion. Id.

For digitally enhanced images, it is unlikely that there will be a witness who can testify how the original scene looked if, for example, a shadow was removed, or the colors were intensified. In such a case, 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[**102] technical evidence under *Rule 702*. Id. Recently, one state court has given particular scrutiny to how this should be done. In State v. Swinton, the defendant was convicted of murder in part based on evidence of computer enhanced images prepared using the Adobe Photoshop software. *268 Conn. 781, 847 A.2d 921, 950-52 (Conn. 2004)*. The images showed a superimposition of the defendants teeth over digital photographs of bite marks taken from the victim's body. At trial, the state called the forensic odontologist (bite mark expert) to testify that the defendant was the source of the bite marks on the defendant. However, the defendant testified that he was not familiar with how the Adobe Photoshop made the overlay photographs, which involved [*562] a multi-step process in which a wax mold of the defendant's teeth was digitally photographed and scanned into the computer to then be superimposed on the photo of the victim. The trial court admitted the exhibits over objection, but the state appellate court reversed, finding that the defendant had not been afforded a chance to challenge the scientific or technical process by which the exhibits had been prepared. The court stated that to authenticate[**103] the exhibits would require a sponsoring witness who could testify, adequately and truthfully, as to exactly what the jury was looking at, and the defendant had a right to cross-examine the witness concerning the evidence. Because the witness called by the state to authenticate the exhibits lacked the computer expertise to do so, the defendant was deprived of the right to cross examine him. *Id. at 951-51*.

Because the process of computer enhancement involves a scientific or technical process, one commentator has suggested the following foundation as a means to authenticate digitally enhanced photographs under *Rule 901(b)(9)*: (1) The witness is an expert in digital photography; (2) the witness testifies as to image enhancement technology, including the creation of the digital image consisting of pixels and the process by which the computer manipulates them; (3) the witness testifies that the processes used are valid; (4) the witness testifies that there has been "adequate research into the specific application of image enhancement technology involved in the case"; (5) the witness testifies that the software used was developed from the research; (6) the witness received [**104] a film photograph; (7) the witness digitized the film photograph using the proper procedure, then used the proper procedure to enhance the film photograph in the computer; (8) the witness can identify the trial exhibit as the product of the enchantment process he or she performed. Edward J. Imwinkelried, Can this Photo be Trusted?, Trial, October 2005 at 54. The author recognized that this is an "extensive foundation," and whether it will be adopted by courts in the future remains to be seen. Id. However, it is probable that courts will require authentication of digitally enhanced photographs by adequate testimony that it is the product of a system or process that produces accurate and reliable results. *FED. R. EVID. 901(b)(9)*.

To prepare properly to address authentication issues associated with electronically generated or stored evidence, a lawyer must identify each category of electronic evidence to be introduced. Then, he or she should determine what courts have required to authenticate this type of evidence, and carefully evaluate the methods of authentication identified in *Rules 901* and *902* , as well as consider requesting a stipulation[**105] from opposing counsel, or filing a request for admission of the genuineness of the evidence under *Rule 36 of the Federal Rules of Civil Procedure*. With this analysis in mind, the lawyer then can plan which method or methods of authentication will be most effective, and prepare the necessary formulation, whether through testimony, affidavit, admission or stipulation. The proffering attorney needs to be specific in presenting the authenticating facts and, if authenticity is challenged, should cite authority to support the method selected.

In this case neither plaintiffs nor defendants provided any authenticating facts for the e-mail and other evidence that they proffered in support of their summary judgment memoranda - they simply attached the exhibits. This complete absence of authentication stripped the exhibits of any evidentiary value because the Court could not consider them as evidentiary facts. This, in turn, required the dismissal, without prejudice, of the cross motions for summary judgment, with leave to resubmit them once the evidentiary deficiencies had been cured.

* * *

Conclusion

In this case the failure of counsel collectively to establish the authenticity of their exhibits [along with other evidentiary issues] rendered their exhibits inadmissible, resulting in the dismissal, without prejudice, of their cross motions for summary judgment. ... Because [we] 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. The Court hopes that the explanation provided in this memorandum order will assist in that endeavor.