

The Next Frontier: Admissibility of Electronic Evidence

Linda L. Listrom
Jenner & Block LLP
Chicago, Illinois

Eric R. Harlan
Shapiro, Sher, Guinot & Sandler
Baltimore, Maryland

Elizabeth H. Ferguson
Stites & Harbison, PLLC
Nashville, Tennessee

Robert M. Redis
McCarthy Fingar LLP
White Plains, New York

In recent years, litigators everywhere have had to learn about information stored in electronic form. In almost any lawsuit, the lawyers and now spend countless hours producing, reviewing, and arguing about this new form of information. In the end, this information is valuable only if, after uncovering it, the trial lawyer knows how to persuade a judge to admit it into evidence. There are no special rules of evidence that govern the admissibility of electronic evidence. In litigation in the federal courts, the Federal Rules of Evidence apply to all types of evidence, including electronic evidence. *See* Manual for Complex Litigation § 11.447 (4th ed. 2004) (“In general, the Federal Rules of Evidence apply to computerized data as they do to other types of evidence”). Any evidence -- regardless of the form that it is in -- must be authentic

and, if it contains hearsay, must fit within one of the exceptions to the hearsay rule. However, it is not always easy to apply the traditional rules to this new form of evidence. *See In re Vinhnee*, 336 B.R. 437, 444-45 (9th Cir. 2005) (bankruptcy panel) (“[t]he paperless electronic record involves a difference in the format of the record that presents more complicated variations on the authentication problem for paper records”). Indeed, some courts have been wary of electronic evidence. *See St. Clair v. Johnny’s Oyster & Shrimp, Inc.*, 76 F. Supp. 2d 773, 774 (S. D. Tex. 1999) (referring to information posted on a website as “inherently untrustworthy”). This article provides analyzes the three principal objections that the proponent of electronic evidence must be prepared to overcome: (1) authenticity (2) hearsay, and (3) best evidence.

I. Authenticity

In order to authenticate or identify evidence, a proponent must offer “evidence sufficient to support a finding that the matter is question is what its proponent claims.” Fed. R. Evid. 901(a). This same authentication requirement applies to electronic evidence. *See* Jack B. Weinstein & Margaret Berger, Weinstein’s Federal Evidence § 901.08 (2d ed. 2007) (“No additional authenticating evidence is required just because the records are in computerized form rather than pen or pencil and paper”).

Rule 901(b) lists ten permitted methods of authentication, which are not exclusive. *See* 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”); *see also Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*, 2004 WL 2367740, at *16 (N.D. Ill. Oct. 15, 2004) (authentication methods listed in Rule 901(b) are “non-exhaustive”); *United States v. Simpson*, 152 F.3d 1241, 1249-50 (10th Cir. 1998) (examples of authentication in the rule are

“merely illustrative” and “are not intended as an exclusive enumeration of allowable methods of authentication”).

While the proponent of electronic evidence need only make a prima facie showing that the evidence is what it purports to be, there are many reported cases in which counsel has failed to make even his minimal showing. *See, e.g. In re Vinhnee*, 336 B.R. 437 (9th Cir. 2005) (bankruptcy panel) (failure to authenticate electronically stored business records); *United States v. Jackson*, 208 F.3d 633, 638 (7th Cir. 2000) (failure to authenticate materials from website); *Lorraine v. Markel American Insurance Co.*, 2007 U.S. Dist. LEXIS (D. Md. May 4, 2007) (dismissing cross motions for summary judgment where parties failed to authenticate electronic evidence); *St. Luke’s Cataract and Laser Inst. v. Sanderson*, 2006 WL 1320242, at *3-4 (M.D. Fla. May 12, 2006) (failure to authenticate website materials); *Uncle Henry’s Inc. v. Plaut Consulting Inc.*, 240 F. Supp. 2d 63, 71-2 (D. Maine 2003), *aff’d*, 399 F.3d 33 (1st Cir. 2005) (failure to authenticate e-mails); *Wady v. Provident Life and Accident Ins. Co. of America*, 216 F. Supp. 2d 1060 (C.D. Cal. 2002) (failure to authenticate website materials); *Amicus Communications v. Hewlett Packard Co.*, 1999 WL 495921, at *16 n. 226 (W.D. Tex. June 11, 1999) (failure to authenticate e-mails); *Hasboro, Inc. v. Clue Computing, Inc.*, 66 F. Supp. 2d 117 (D. Mass. 1999) (failure to authenticate e-mails); *Indianapolis Minority Contractors Ass’n. v. Wiley*, 1998 WL 1988826, at * 7 (S.D. Ind. May 13, 1998), *aff’d*, 187 F.3d 743 (7th cir. 1999) (failure to authenticate computer records). As one federal court recently observed, referring to electronic evidence, “[T]he 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.” *Lorraine*, 2007 U.S. Dist. LEXIS 33020, at *31.

In the discussion that follows we demonstrate how the trial lawyer can apply the authentication methods listed in Rule 901(b) to four common types of electronic evidence: (1) e-mails, (2)

website postings, (3) transcripts of chat room conversations and instant messages, and (4) data stored in electronic form.

A. E-mails

The simplest way to authenticate an e-mail is to offer the testimony of the person with personal knowledge of the e-mail, such as the person who drafted and sent it. Rule 901(b)(1) permits authentication by “[t]estimony that a matter is what it is claimed to be.” *See United States v. Safavian*, 435 F. Supp. 2d 36 (D.D.C. 2006) (e-mail can be authenticated by the testimony of a witness with knowledge). However, where this method of authentication is not available, there are several other common methods of authentication.

Rule 901(b)(4) permits authentication by “Distinctive characteristics,” including “Appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances. The commentary to the rule provides several examples of this kind of authentication:

“Thus a document or telephone conversation may be shown to have emanated from a particular person by virtue of its disclosing knowledge of facts known peculiarly to him....similarly, a letter may be authenticated by content and circumstances indicating it was in reply to a duly authenticated one. Language patterns may indicate authenticity or the opposite....

Federal Rule of Evidence 901, Advisory Committee’s Notes, Example (4). This is method of authentication is often referred to as authentication by “circumstantial evidence.” Weinstein at §901.03[8]. This method has been successfully used to authenticate e-mails. *See United States v. Siddiqui*, 235 F.3d 1318 (11th Cir. 2000); *United States v. Safavian*, 435 F. Supp. 2d 36 (D.D.C. 2006); *Massimo v. State of Texas*, 144 S.W.3d 210, 216-7

(Tex. App. 2004).

In *Siddiqui* the government introduced into evidence a series of e-mails that the defendant purportedly sent to third party witnesses. The recipients testified that they received the e-mails, but the defendant argued that the government had failed to prove that he was the person who sent them. Relying upon Rule 901(b)(4), the court of appeals concluded that several “distinctive characteristics” demonstrated that the defendant sent these e-mails. *Id.* at 1322. Each e-mail bore the defendant’s e-mail address and the recipient of one of the e-mails testified that when he clicked on “reply” to the e-mail, his e-mail system displayed the defendant’s e-mail address. In the e-mails the sender referred to details about the defendant’s illegal conduct. The e-mails referred to the author as “Mo,” a nickname for the defendant. Finally, the recipients testified that they spoke by phone with the defendant shortly after receiving the e-mails and in these conversations he repeated the content of the e-mail. The court held that these factors were sufficient to authenticate the e-mail.

In *Safavian*, the e-mails showed the e-mail address of the sender and most also showed the name of the person connected to that e-mail address, such as David.Safavian@mail.house.gov. Frequently, the e-mails contained the name of the sender or the recipient in the bodies of the e-mail, in the signature blocks at the end of the e-mail, in the “To:” and “From:” headings, and by the signature of the sender. The e-mails also referred to various personal and professional matters known to the defendant.

One court has suggested that any electronic record can be authenticated under Rule 901(b)(4) using metadata. *See Lorraine v. Markel American Insurance Co.*, 2007 U.S. Dist. LEXIS 33020, at *48 (D. Md. May 8, 2007). Metadata is “data about data.” *See, e.g., Netword, LLC v. Central Corp.*, 242 F.3d 1347, 1354 (Fed. Cir. 2001). The Advisory Committee’s Note to the 2006 Amendments to Federal Rule of Civil Procedure 26(f) refers to

metadata as “information describing the history, tracking, or management of an electronic file.” Examples of such transactional information 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, date of last metadata modification); file permissions (e.g., who can read the data, who can write to it, who can run it).” *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age*, App. F n.1 (The Sedona Conference Working Group Series, Sept. 2005 Version). As the court observed in *Lorraine*, “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).” *Id.* at *48.

When “distinctive characteristics” are not available to authenticate an e-mail, it may also be authenticated under Rule 901(b)(3), which permits authentication by “[c]omparison by the trier of fact or by expert witnesses with specimens which had already been authenticated.” This method was used to authenticate some of the e-mails in *United States v. Safavian*, 435 F. Supp. 2d 26 (D.D.C. 2006). For example, some of the e-mails in that case contained the address MerrittDC@aol.com, but neither the e-mail heading nor the contents identified the person who used that e-mail address. However, when the court compared this e-mail to other e-mails that were properly authenticated, it was clear that this e-mail address was used by the defendant. For example, another e-mail that had been properly authenticated under Rule 901(b)(4) was sent by MerrittDC@aol.com and included a signature with the defendant’s name and the name of his business.

An e-mail may also be self-authenticating under Rule 902, which lists twelve types of documents which may be authenticated without the use of extrinsic evidence. One method of self

authentication that is particularly relevant to e-mails is 902(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 matter set forth by, or from information transmitted by, a person with knowledge of those matters; (B) was kept in the court of the regularly conducted activity; and (C) was made by the regularly conducted activity as a regular practice.

In effect, Rule 902(11) requires the proponent to establish all of the elements of the business records exception to the hearsay rule. *See Rambus, Inc. v. Infineon Technologies AG*, 348 F. Supp. 2d 698, 710 (E.D. Va. 2004) (Rule 902(11) is the “functional equivalent of testimony offered to authenticate a business record” under Rule 803(6)); *In re Vinhnee*, 336 B.R. 437, 444 (9th Cir. 2005) (bankruptcy panel) (because the elements of Rule 902(11) and Rule 803(6) are identical, “the authenticity analysis is merged into the business records analysis”). However, as explain below, in the section on hearsay, a proponent should not assume that all e-mails will qualify as business records.

Finally, it is important to remember that Rule 901 does not list all of the appropriate methods for authentication. For example, some courts have held that e-mails produced by a party in litigation are presumed to be authentic. *See Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1153-54 (C.D. Cal. 2002); *Indianapolis Minority Contractors Ass’n v. Wiley*, 1998

WL 1988826, at*6 (S.D. Ind. May 13, 1998); *Maljack Productions, Inc. v. Good Times Home Video Corp.*, 81 F.3d 881, 889 n. 12 (9th Cir. 1996).

B. Websites

A business letter is authentic if it contains the letterhead or logo of the company which originated the letter. *See, e.g. Denison v. Swaco Geograph Co.*, 941 F.2d 1416, 1423 (10 Cir. 1991). By analogy, it would seem reasonable to assume that a website which contains a company logo and can be found at the URL address for that company is also authentic. However, some courts have been skeptical of information posted on websites. Weinstein's Federal Evidence § 901.08[2]. In a widely quoted case one judge remarked,

While some look to the Internet as an innovative vehicle for communication, the Court continues to warily and wearily view it largely as one large catalyst for rumor, innuendo, and misinformation....Anyone can put anything on the Internet. No web-site is monitored for accuracy and *nothing* contained therein is under oath or even subject to independent verification absent underlying documentation. Moreover, the Court holds no illusions that hackers can adulterate the content on *any* web-site from *any* location at *any* time.”

St. Clair v. Johnny's Oyster & Shrimp, Inc., 76 F. Supp. 2d 773, 774-75 (S. D. Tex. 1999); *see also Terbush v. United States*, 2005 WL 3325954, at *5 n. 4 (E.D. Cal. Dec. 7, 2005) (“Information on internet sites presents special problems of authentication.”) For this reason, courts have consistently held that evidence obtained from websites is not self-authenticating under Rule 902. *See Sun Protection Factory, Inc. v. Tender Corp.*, 2005 WL 2484710 (M.D. Fla. 2005); *Ashworth v. Round Lake Beach Police Dept.*,

2005 WL 1785314 (N. D. Ill. 2005); *In re Homestore.com, Inc. Securities Litigation*, 347 F.Supp. 2d 769, 782-83 (C.D. Cal. 2004).

The typical method of authentication for website postings is Rule 901(b)(1), which permits authentication through the testimony of a “witness with knowledge.” While the courts agree that website evidence can be authenticated under Rule 901(b)(1) by a person with knowledge, they disagree on how much knowledge is required.

Several courts have held that the proponent must offer the testimony from the website’s owner. *See United States v. Jackson*, 208 F.3d 633, 637 (7th Cir. 2000) (proponent of information posted on white supremacist website must show that website sponsor posted the information, “as opposed to being slipped onto the groups’ websites by [the defendant] herself, who was a skilled computer user”); *Novak v. Tucows, Inc.*, 2007 U.S. Dist. LEXIS 21269, at *5 (E.D.N.Y. March 26, 2007). (website printouts are not authenticate because the plaintiff offered no testimony or sworn statements by an employee of the companies hosting the sites); *St. Luke’s Cataract and Laser Inst. v. Sanderson*, 2006 WL 1320242 at *2-4 (M.D. Fla. May 12, 2006); *Illusions-Dallas Private Club, Inc. v. Steen*, 2005 WL 1639211, at*10 (N. D. Tex. July 13, 2005), *rev’d on other grounds*, 482 F.3d 299 (5th Cir. 2007) (affidavit from attorney for party that he obtained a document from the website is insufficient, because “there is no showing of personal knowledge that the studies are what they are claimed to be”); *Costa v. Keppel Singmarine Dockyard PTE, Ltd.*, 2003 U.S. Dist. LEXIS 16295, at *9 n.74 (C.D. Cal. April 25, 2003) (affidavit stating that affiant personally downloaded certain pages from defendant’s website was insufficient, because party did not proffer “the testimony of a [defendant] representative attesting that the information was placed there by the corporation”) *Wady v. Provident Life and Accident Insurance Co. of America*, 216 F. Supp. 2d 1060, 1064-65 (C. D. Cal. 2002) (holding that affiant

cannot authenticate website postings, because he has “no personal knowledge of who maintains the website, who authored the documents, or the accuracy of their contents”); *see also Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*, 2004 WL 2367740, at *16 (N.D. Ill. Oct. 15, 2004) (finding affidavit from website owner to be sufficient to authenticate printout).

However, other courts had held that printouts and postings from websites are admissible, even in the absence of testimony from the website’s owner. *See United States v. Standring*, 2006 WL 689116, at *3 (S. D. Ohio March 15, 2006); *Moose Creek, Inc. v. Abercrombie & Fitch Co.*, 331 F. Supp. 2d 1214, 1225 n. 4 (C.D. Cal. 2004), *aff’d*, 114 Fed. Appx. 921 (9th Cir. 2004) (unpublished opinion); *Perfect 10, Inc. v. Cybernet Adventures, Inc.*, 213 F. Supp. 2d 1146, 1153-54 (C.D. Cal. 2002); *Johnson-Wooldridge v. Wooldridge*, 2001 WL 838986, at *4-5 (Ohio Ct. App. 2001). In each of the foregoing cases, the proponent of the website evidence offered the testimony of (or an affidavit from) someone who personally visited a website and printed out information he or should found there. In each case the court found, over the objections of opposing counsel, that this was sufficient to authenticate the document. However, in *Perfect 10* and *Standring* the proponent also authenticated the evidence under Rule 901(b)(4) by demonstrating that the website pages contained the internet domain address from which the image was printed and the date on which it was printed.

If the website belongs to a government agency, the proponent may be able to authenticate the posting under Rule 901(b)(5). Under this provision, “Books, pamphlets, or other publications purporting to be issued by public authority” are self-authenticating and the proponent need not offer any extrinsic evidence of authenticity. *Id.* One court has concluded, based on this rule, that information posted on government websites is self-authenticating. *Lorraine v. Markel American Insurance Co.*, 2007 U.S. Dist. LEXIS 330220, at *18 (D. Md. May 8, 2007); *but see*

State v. Davis, 10 P.3d 977, 1010 (Wash. 2000) (refusing to admit population statistics taken from state agency's website that had not been authenticated).

In summary, based on the conflicting authority, it is difficult to predict how a particular court will rule on the authenticity of website evidence. It will almost certainly be sufficient for the proponent to authenticate a website through the testimony of the web master or other knowledgeable person employed by the website owner. Whenever possible, the litigant who plans to offer evidence from a website should lay the necessary foundation by deposing the web master or other knowledgeable employee site's owner. Where that is not possible, the litigant may be able to authenticate the evidence by relying upon distinctive characteristics, such as the URL address on the printout, the date on the printout, or other distinctive features of the website content which suggest that the site is authentic. In order to improve the chances that the evidence will be admitted, the proponent should identify as many distinctive characteristics as possible.

C. Chat Rooms and Instant Messages

Whenever a litigant seeks to introduce into evidence transcripts of chat room discussions or instant messages, the challenge usually is proving the identity of the persons in the conversation. In chat rooms users typically use screen names that often reveal little if anything about the user's identity. In this situation the transcript almost always must be authenticated under Rule 901(b)(4), using circumstantial evidence. *See United States v. Tank*, 200 F.3d 627 (9th Cir. 2000) (chat room discussions); *United States v. Simpson*, 152 F.3d 1241 (10th Cir. 1998) (chat room discussions); *People v. Von Gunten*, 2002 Cal. App. Unpub. LEXIS 2361 (Cal. Ct. App. April 4, 2002); *In Re F.P., a Minor*, 878 A.2d 91, 95 (Sup. Ct. Pa. 2005) (instant messages). However, in these cases the courts disagree on how much circumstantial evidence is required.

The leading case on authentication of chat room conversations is *Tank*, a criminal case in which the defendant was charged with conspiracy and illegal distribution of child pornography. The defendant belonged to a private password-protected internet chat room called the Orchid Club whose members discussed, traded and produced child pornography. While online in the chat room Orchid Club members traded digital pornographic images of children. Another member of the club, Ronald Riva, was arrested on a child molestation charge. When police searched his home and computer files they found that Riva had saved all of the Orchid Club's chat room discussions as text files in his computer. These chat room discussions implicated other members of the club, including the defendant Tank. At trial the government introduced these chat room logs into evidence over the objection of the defendant. On appeal the defendant argued that the government failed to authenticate these records. The court of appeals disagreed, concluding that the government authenticated these records in two ways. *Id.* at 630-31. First, Riva testified as a government witness. He explained how he had created the logs and stated that the printouts were an accurate record of the chat room discussions among members of the Orchid Club. *Id.* at 630. Second, the court relied upon certain distinctive characteristics in the chat room log. The defendant Tank admitted the he used the screen name "Cessna." Several co-conspirators also testified that Tank used this screen name at that when they arranged a meeting with the person who used the name "Cessna" the defendant showed up. The name "Cessna" appeared throughout the printouts. *Id.* at 630-31.

In *Simpson* the defendant, who was convicted of receiving child pornography, argued that the trial court erred in admitting a computer printout of a chat room discussion between a police detective and an individual who used the screen name "Stavron." The government contended that "Stavron" was the defendant, but the defendant argued that the government had not authenticated the

printout. The Court of Appeals disagreed. During the chat room discussion the individual using the name “Stavron” told the detective that his name was “B. Simpson” and gave the correct street address. “Stavron” also used an e-mail address which belonged to the defendant Simpson. When the police executed a search warrant at the defendant’s home they found a piece of paper, lying near his computer, containing the name, street address, e-mail address and telephone number that the detective had given the defendant during the chat room discussion. Based on this evidence, the court concluded that the exhibit had been properly authenticated.

In re F.P., a Minor the defendant, a juvenile, was charged with assault. The victim testified that the defendant was angry, because he believed that the victim had stolen something from him. The trial court admitted into evidence transcripts of instant messages between the victim and an individual who used the screen name “Icp4Life30.” In these messages, “Icp4Life30 threatened to beat up the victim. On appeal, the defendant argued that there was no evidence that he was the author of these messages. The appellate court concluded that the contents of the transcripts demonstrated their authenticity. *Id.* at 95. During their first conversation the victim asked, “who is this,” and “Icp4Life 30” responded with the defendant’s first name. In addition, in several of the messages “Icp4Life30” accused the victim of stealing from him and referred to meetings that he and the victim had had with school authorities. *Id.*

However, in *People v. Van Guten*, the appellate court found that there was insufficient evidence to authenticate the identity of a person who sent an instant message. In this case the defendant, who was charged with assault with a deadly weapon, offered the transcript of an instant message between a female friend and a person using the screen name “BukaRoo2.” In this message, BukaRoo2 admitted that he had stabbed one of the defendant’s friends during a fight and threatened to “finish the job.” The

defendant contended that BukaRoo2 was the victim and that these messages proved that the defendant had acted in defense of himself and his friend. At defense counsel attempted to authenticate the instant message, using the testimony of the female friend. She testified that she had included the name screen name BukaRoo2 on a list of people from whom she would accept instant messages after a friend of the victim provided her with this screen name. She had several online conversations with BukaRoo2 and the content of these conversation suggested to her that BukaRoo2 was the victim. However, she was unable to be specific. The appellate court agreed that this testimony was insufficient to authenticate the instant message. Distinguishing *Tank*, the trial court emphasized that the witness could not any identify particular facts referenced in this instant messages known only to her and the victim. *Id.* at *8.

D. Data Stored in Electronic Form

Data stored in electronic form usually must be authenticated under Rule 901(b)(9), which permits authentication through “[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.” *Id.* As the Advisory Committee’s Note to the rule explains, this provision, “is designed for situations in which the accuracy of the result is dependent upon a process or system which produces it.” *Id.* Theoretically, any information that passes through a computer network -- including e-mails -- must be authenticated under Rule 901(b)(9). However, in practice the use of e-mail and some other forms of technology is so ubiquitous that in practice courts have not questioned the reliability of these systems. *See* Paul R. Rice, *Electronic Evidence, Law and Practice* 256 (2005) (suggesting that e-mail systems are so widely used that courts should take judicial notice of their reliability); *see also* Fed. R. Evid. 901, Advisory Committee’s Note, Example (9) (Rule 901(b)(9) “does not, of course, foreclose taking judicial notice of the accuracy of the process or system.”).

If the proponent of data stored in electronic form offers this evidence for its truth, he or she must also prove that it fits within one of the exceptions to the hearsay rule. Most proponents rely on the business records exception to the hearsay rule. In order to lay the necessary foundation under Federal Rule 803(6) the proponent must prove that the records are trustworthy. See Fed. R. Evid. 803(6) (records of regularly conducted activity are admissible “unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness.”) As a practical matter, the proponent usually meets the authentication requirement of Rule 901 by proving that the computerized data is a business record. Weinstein’s Federal Evidence, §900.06[2][b]. In other words, the proof that is used to establish that a computer system is trustworthy under Rule 803(6) is usually identical to the proof used to show that a computer system produces an accurate result” under Rule 901(b)(9). The necessary foundation for computerized data as business records is discussed in the next section.

II. Hearsay

Hearsay is “a statement . . . offered in evidence to prove the truth of the matter asserted.” Fed. R. Evid. 801(c). If electronic evidence is offered for its truth, the proponent must be prepared to meet one of the exceptions to the hearsay rule. See Fed. Rule Evid. 803. Below, we discuss when the hearsay rule applies to electronic evidence and some of the most common exceptions to the rule.

A. E-mail

E-mail communications sent by party opponent are not hearsay under 801(d)(2), provided of course, that the proponent has demonstrated that it was the party opponent who authored the e-mail. See *Perfect 10, Inc. v. Cybernet Ventures, Inc.* 213 F. Supp. 2d 1146, 1155 (C.D. Cal. 2002); *United States v. Siddiqui*, 235 F.3d 1318, 1323 (11th Cir. 2000); *United States v. Sprick*, 233 F.3d 845, 852 (5th Cir. 2000); *United States v. Safavian*, 345 F. Supp. 2d 36, 43-44 (D.D.C. 2006); but see *Ermolaou v. Flipside*,

Inc. 2004 WL 503758, at *6 (S.D.N.Y. March 15, 2004) (e-mail was not an admission because it was the product of computer error). In fact, even if the e-mail was authored by someone else, a party may have “manifested an adoption or belief its truth,” Fed. R. Evid. 801(d)(2)(B) by forwarding the e-mail to others, making it an adoptive admission under Rule 801. *See Sea-Land Serv., Inc. v. Lozen Int’l, LLC*, 285 F.3d 808, 821 (9th Cir. 2002); *Safavian*, 345 F. Supp. 2d at 43-44.

If the e-mail was not authored by a party opponent, it may qualify as a business record under Rule 803(6) which provides as follows:

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...

Id. While an e-mail may qualify as a business record under Rule 803(6), a litigant should not assume that all e-mails generated by employees of a business constitute business records. As one court has explained:

It is essential for the exception to apply that it was made in furtherance of the business’ needs, [and] not for the personal purposes of the person who made it. Given the fact that many employees use the computers where they work for personal as well as business reasons, some care must be taken to analyze whether the business record exception is applicable, especially to e-mail.

Lorraine v. Markel American Insurance Co., 2007 U.S. Dist. LEXIS 33020, at *36 (D. Md. May 4, 2007).

Using this same analysis, a number of courts have held that e-mails are not business records. See *Monotype Corp. v. Int'l Typeface Corp.*, 43 F.3d 443, 450 (9th Cir. 1994) (“E-mail is far less of a systematic business activity than a monthly inventory printout”); *Westfed Holdings, Inc. v. United States*, 55 Fed. Cl. 544, 566 (2003), *rev'd on other grounds*, 407 F.3d 1352 (Fed. Cir. 2005) (“The fact that e-mail was used as a regular form of communication does not alone satisfy the business records exception”); *State v. Microsoft*, 2002 WL 649951, at *2 (D.D.C. April 12, 2002) (refusing to admit e-mail as a business record because there was no evidence that it was the regular practice of a company’s employees to write and maintain such e-mails); see also *Rambus, Inc. v. Infineon Technologies AG*, 348 F. Supp. 2d 698, 705-06 (E.D. Va. 2004) (“The fact that an employee ‘routinely’ takes meeting notes and keeps them is quite different that whether a company policy directs the employee to do so”); *United States v. Ferber*, 966 F. Supp. 90, 98-99 (D. Mass. 1997).

Ferber illustrates the problem. In that case the government attempted to introduce into evidence an e-mail authored by the employee of a brokerage firm. The employee testified that it was his routine practice to prepare e-mails like this. The trial court refused to admit the evidence, concluding that, “while it may have been [the employee’s] practice to make such records, there was not sufficient evidence that Merrill Lynch required such records to be maintained.” *Id.* at 98. This was fatal, because “in order for a document to be admitted as a business record, there must be some evidence of a business duty to make and regularly maintain records of this type.” *Id.* In this case there was no evidence that the witness’s employer, the broker firm, required its employees to make and maintain e-mail messages. *Id.* at 99. See also Fed. R. Evid. 803(6) (requiring proof that the document was “kept in the course of regularly conducted activity” and that it was “the regular

practice that that business activity” to create the document).

In short, if a proponent plans to offer an e-mail under the business records exception, he or she must lay a foundation that it was the policy of the business to require employees to prepare and keep e-mails.

B. Websites

When the trial lawyers plans to offer a printout from a website into evidence, it is particularly important that he or she analyze whether the website is hearsay. If the website does nothing more than reproduce information that meets some exception to the hearsay rule, it is not objectionable. For example, in *Florida Conference Ass’n of Seventh-Day Adventists v. Kyriakides*, 151 F. Supp. 2d 1223, 1225-26 (C.D. Cal. 2001), the court held that the act of placing SEC reports, which qualified as public records, on a website is not hearsay, because “[o]nly non-verbal conduct which is intended as an assertion is hearsay.” See also P. Rice *Electronic Evidence, Law and Practice* 279-80 (2005) (“the mechanical recording of data on a Web page on the Internet does not create hearsay”). If the information posted on a website is offered to prove that the information was posted, rather than the truth of the information, it is not hearsay. See *United States v. Standring*, 2005 WL 3981672, at *2; *Perfect 10, Inc v. Cybernet Ventures, Inc.*, 213 F. Supp. 2d 1146, 1155 (C. D. Cal. 2002); *Telewizka* at *4. If the website belongs to a party opponent, the information posted there may constitute an admission, provided, of course, that a foundation has been laid that the website is what it purports to be. See *Vam Westrienen v. Americontinental Collection Corp.*, 94 F. Supp. 2d 1087, 1109 (D. Ore. 2000).

If the trial lawyer is satisfied that the website contains hearsay, he or she must lay a foundation for one of the exceptions of the hearsay rule.

Information posted on the website of a government entity may qualify as a public record or report under Rule 803(8). Some courts have found that website information fits within this exception. See *EEOC v. E.I. DuPont DeMours & Co.*, 2004 WL 2347559, at *1 (E.D. La. 2004), *aff'd*, 480 f.3d 724 (5th Cir. 2007) (data from U.S. Census Bureau website qualifies as a public record); *Chapman v. San Francisco Newspaper Agency*, 2002 WL 31119944, at *3 (N.D. Cal. Sept. 20, 2002) (holding that printout from U.S. Postal Service website is admissible as a public record); *Johnson-Wooldridge v. Wooldridge*, 2001 WL 838986, at *4 (Ohio App. 2001) (holding that printouts from the state board of education website were admissible as public records). However, consistent with the judicial skepticism of the accuracy of website information, at least one court has found that website information is not admissible under Rule 803(8). See *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, 76 F. Supp. 2d 773, 774-75 (S.D. Tex. 1999) (information posted on Coast Guard website is not admissible under any hearsay exception, because “[a]nyone can put anything on the internet”).

A website may also contain “Market quotations, tabulations, lists, directories, or other published compilations, generally used and relied upon by the public or persons in particular occupations.” Fed. R. Evid. 803(17). See *Elliot Assocs., L.P. v. Banco de la Nacion*, 194 F.R.D. 116, 121 (S.D.N.Y. 2000) (prime interest rates from website of Federal Reserve Board and Bloomberg); *Irby-Greene v. M.O.R., Inc.*, 79 F. Supp. 2d 630, 636, n. 22 (E.D. Va. 2000) (value of vehicle as listed on the Kelley Blue Book web site); *State v. Erikstad*, 620 N.W.2d 136, 145 (N.D. 2000) (same).

Finally, the information on a website may contain records of regularly conducted activity under Rule 803(6), the business records exception to the hearsay rule. We have been unable to find any case in which a court admits, or refuses to admit, information from a website under the business records exception. However, at

least one court has suggested that it may be possible for the proponent to lay the necessary foundation qualifying this information as a business record. See *Border Collie Rescue, Inc. v. Ryan*, 418 F. Supp. 2d 1330, 1350 n. 16 (M.D. Fla. 2006). Another court has admitted records kept and maintained by the State of New York on its official government website as a business record. See *Proscan Radiology of Buffalo v. Progressive Cas. Ins. Co.*, 820 N.Y.S.2d 845 (City Ct. of N.Y. 2006). But see *United States v. Jackson*, 208 F.3d 633, 637 (7th Cir. 2000) (holding that information posted on a website is not business record of the Internet Service Provider).

C. Data Stored in Electronic Form

If the electronic data was produced by a business, the proponent of the evidence will typically attempt to overcome the hearsay objection by proving the elements of the business records exception to that rule.

A number of courts have held that the necessary foundation under Rule 803(6) is the same for computerized business records as for paper records. See e.g. *Sea-Land Serv., Inc. v. Lozen Int'l*, 285 F.3d 808, 819-820 (9th Cir. 2002) (holding that “it is immaterial that the business record is maintained in a computer rather than in company books” and that “a data compilation, in any form” is admissible as long as the proponent lays a proper foundation under Rule 803(6)); *United States v. Fuji*, 301 F.3d 535 (7th Cir. 2002) (computerized records were admissible as business records on a showing that the data reflected in the printouts was kept in the ordinary course of business); *United States v. Hutson*, 821 F.2d 1015, 1019 (5th Cir. 1987) (holding that computer records are admissible if the requirements of Rule 803(6) have been met).

Courts have rejected arguments that the witness laying the foundation must attest to the accuracy of either the data or the computer system. See *United States v. Salgado*, 250 F.3d 438, 453

(6th Cir. 2001) (expert testimony on the mechanical accuracy of the computer was not required); *United States v. Moore*, 923 F.2d 910, 915 (1st Cir. 1991) (rejecting argument that the proponent must offer some evidence of trustworthiness beyond the foundational requirements of 803(6)); *Huston*, 821 F.2d 1015, 1020 (5th Cir. 1987) (foundational witness need not testify about the accuracy of the data). Even when opposing counsel demonstrates inaccuracies in the data, courts have held that these inaccuracies go to the weight of the evidence and not its admissibility. See *United States v. Catabran*, 836 F.2d 453, 458 (9th Cir. 1988).

However, the Manual for Complex Litigation cautions:

In general the Federal Rules of Evidence apply to computerized data as they do to other types of evidence. Computerized data, however, raise unique issues concerning accuracy and authenticity. Accuracy may be impaired by incomplete data entry, mistakes in output instructions, programming errors, damage and contamination of storage media, power outages, and equipment malfunctions. The integrity of data may also be compromised in the course of discovery by improper search and retrieval techniques, data conversion or mishandling. The proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy.

Manual for Complex Litigation §11.447 (4th ed. 2004)/

For these reasons, at least one court has held that the proponent of computerized data must do more than meet the foundational requirements in Rule 803(6). See *In re Vinhnee*, 336 B.R. 437 (9th Cir. 2005) (bankruptcy appellate panel). In that case a credit card company used a custodian of records to authenticate

computer printouts showing the account balances on the debtor's credit cards. The custodian testified that the entries in the account records were made at or about the time of the transactions, that the records were kept in the regular course of business, and that the regular practice was to retain the records. The witness also explained that the records were retained electronically. The trial court held that, because the records were maintained electronically, the credit card company needed to authenticate the hardware and software used to generate the printout. When the credit card company failed to produce a witness who could lay this foundation, the trial court refused to admit the electronic records into evidence and ruled against the credit card company.

The court of appeals affirmed. The court held that, in addition to proving that the computerized records were records of regularly conducted activity under Rule 803(6), the burden was on the proponent to prove that the records were "authentic." In order to prove authenticity, the proponent must prove "what has, or may have, happened to the record in the interval between the time when it was placed in the files and the time of trial. In other words, the record being proffered must be shown to be an accurate representation of the record that was originally created." *Id.* at 444. According to the court, the necessary foundation

extend[s] 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, as pertinent to the question

of whether records have been changed since their creation.

Id. at 445. Quoting the Manual for Complex Litigation, the court observed that “a proponent of computerized evidence has the burden of laying a proper foundation by establishing its accuracy.” *Id.* The court also quoted with approval, an eleven-step foundation for computer records, advocated by one commentator:

1. The business uses a computer;
2. The computer is reliable;
3. The business had 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; and
11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.

Id. at 446, quoting Imwinkelried, *Evidentiary Foundations* §4.03[2] (5th ed. 2002)

One court summarized the state of the law on this subject as follows:

[S]ome courts will require the proponent of electronic business records or e-mail evidence to make an enhanced showing in addition to meeting each element of the business records exception.

These courts are concerned that the information generated for use in litigation may have been altered, changed or manipulated after its initial input, or that the programs and procedures used to create and maintain the records are not reliable or accurate. Others will be content to view electronic business records in the same light as traditional 'hard copy' records, and require only a rudimentary foundation. Unless counsel knows what level of scrutiny will be required, it would be prudent to analyze electronic business records that are essential to his or her case by the most demanding standard.

Lorraine v. Markel American Insurance Co., 2007 U.S. Dist. LEXIS 33020, at *149.

III. The Best Evidence Rule

The best evidence rule ordinarily will not bar the admission of electronic evidence. Under Federal Rule of Evidence 1002, "To prove the content of a writing, recording, or photograph, the original . . . is required." However, under Rule 1001(3), "if data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately is an 'original.'"

ABOUT THE PRESENTER(S)

Gregory P. Joseph

Mr. Joseph is a former chair of the Section of Litigation. Before starting his own firm, he chaired the Litigation Department of Fried, Frank, Harris, Shriver & Jacobson in New York. By appointment of Chief Justice William Rehnquist, Mr. Joseph served on the Advisory Committee on the Federal Rules of Evidence from 1993-1999. He has also served as Chair of the New York State Courts' Committee of Lawyers to Enhance the Jury Process and as Co-Chair of the Third Circuit Task Force on Selection of Class Counsel. In a 2006 world survey conducted by London-based *Who's Who Legal*, Mr. Joseph was rated one of the 10 most highly regarded commercial litigators in the world. Mr. Joseph is also a fellow in the American College of Trial Lawyers. He is an honors graduate of the University of Minnesota Law School.

Sheldon M. Finkelstein

Mr. Finkelstein is a partner in the Newark, New Jersey firm of Podvey, Meanor, Catenacci, Hildner, Coccoziello & Chattman. Mr. Finkelstein's practice focuses on complex commercial litigation, RICO, securities litigation, creditor's rights litigation, labor and employment litigation and business crimes litigation. Mr. Finkelstein has chaired several divisions within the Section of Litigation and has served as Co-Chair of the Section's Trial Practice and Pre-trial Practice and Discovery Committees. He has written several articles that have been published in the Section's magazine, *Litigation*. Mr. Finkelstein received his J.D. from Columbia University.

Linda L. Listrom

Ms. Listrom is a partner in the Chicago office of Jenner & Block LLP. Her practice focuses on complex business litigation. In 2005 and 2006 Ms. Listrom was named by *Law Dragon* magazine as one of the 500 outstanding lawyers in the United States. Ms. Listrom serves as Co-Chair of the Section of Litigation's Trial Evidence Committee and for four years served as Co-Chair of its Trial Practice Committee. She is a Fellow in the American College of Trial Lawyers. Ms. Listrom received her J.D. from Harvard Law School.