Prepare for the Most Demanding Standard

The Admissibility of Electronically Stored Information

By Dale Conder, Jr.

Learn what to look for, what questions to ask during discovery, and how to use ESI to your advantage.

It is late on Friday and, after working for months on a big case that was just settled, you are looking forward to a weekend away from the office. As you finish up a few last-minute items before leaving the office, you are suddenly brought back to reality by a ringing phone—your phone. According to the caller I.D., the call is from one of the senior partners in your firm. She has practiced law for almost 30 years and is legendary in your firm. With some hesitation, you answer the phone.

She has a problem, and she thinks you can help her. She explains that she has several cases of files with a lot of electronically stored information (ESI), and she needs some quick research outlining the admissibility of this "stuff." According to her, the files include everything from chat room logs to webpage content to instant messaging. Good thing you went to all of those seminars on electronic discovery. At least you know what ESI means, because on a Friday night, every little bit helps.

A Review of the Rules of Evidence

If the issue in a case involves a constitutional provision, a statute, or the application of a rule or regulation, it is always wise to review the applicable constitutional provision, statute, rule or regulation before deciding how best to proceed. The same is true when it comes to the admissibility of evidence, especially in the world of ESI.

The Federal Rules of Evidence do not specifically address the admissibility of ESI, but the rules are intended to promote "growth and development of the law of evidence" as our world changes and technology advances. Fed. R. Evid. 102. Certainly the evidence, whether it is ESI or a plaintiff's handwritten diary, must be relevant. If the "evidence [has] any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence[,]" it is relevant. Fed. R. Evid. 401.

Once you have decided the ESI satisfies Rule 401, your next step is to decide how to authenticate the evidence. Simply put, can sufficient evidence be identified to establish that the evidence to be authenticated

■ Dale Conder, Jr., is a member of Rainey, Kizer, Reviere & Bell, P.L.C., in Jackson, Mississippi. He has significant experience in the areas of employment law (representing employers only), personal injury litigation, federal civil rights litigation and appellate advocacy, and has represented a number of police departments and municipalities in 42 U.S.C. §1983 litigation. In addition to DRI, Mr. Conder is a member of the Jackson-Madison County Bar Association, the Tennessee Bar Association, and the Tennessee Defense Lawyers Association.

is what its proponent claims it is? FED. R. EVID. 901(a). In most cases, the parties can stipulate that the evidence is what one party claims it to be. For example, in a car wreck case, parties can agree the car depicted in particular photographs represent the condition of the car before and after the wreck or particular medical records are records from the doctor regarding the plaintiff's treatment. But, dealing with ESI may not be as cut-and-dried.

Just because document evidence, such as ESI, is authentic, does not mean the information in the documents is true. Establishing the authenticity of ESI and the truth of the information contained in the files are two different matters. *See United States v. Brown*, 688 F.2d 1112, 1116 (7th Cir. 1982). In *Brown*, the defendant produced documents to a grand jury. Following his indictment, the documents were admitted into evidence at his trial despite his refusal to testify as to the authenticity of the documents. On appeal, he challenged the admissibility of the records on the grounds that they were not properly authenticated and their admission violated his right against self-incrimination. The court held that (1) his production of the records to the government was sufficient to authenticate the records, and (2) his Fifth Amendment right against self-incrimination was not violated because authentication is not the same as vouching for the accuracy of the information in the documents. *Id.*

Rule 901(b) provides a list of ways in which evidence can be authenticated. But the list is not exhaustive and is intended only to illustrate ways in which Rule 901 can be satisfied. FED. R. EVID. 901(b). Rule 902 sets forth 12 situations in which extrinsic evidence of authenticity is not required "as a condition precedent to admissibility…." FED. R. EVID. 902. The codification of these 12 areas, however, does not prohibit your opponent from contesting the authenticity of a document. FED. R. EVID. 902 (1972 advisory committee's notes).

The next hurdle that must be cleared is hearsay. You have a hearsay problem if the real witness is not the person in the witness chair and you are offering the statement to prove the truth of a matter. For example, you are defending an employer in a sex discrimination case, and the plaintiff's attorney calls a witness to describe an incident he saw. So far all is well, at least from the point of view of hearsay. Then your opponent asks the witness about the contents of an e-mail he received from another employee regarding what she saw. It is time to object (unless the statement fits into one of Rule 803's 23 exceptions to the rule against admitting hearsay). If the real witness, or declarant, is unavailable, the hearsay may still be admissible if Rule 804's hearsay exceptions are satisfied. But even if the evidence does not fit within Rules 803 or 804, all is not lost; you still might be able to fit the evidence into the residual exception found at Rule 807.

Finally, our review will bring us to the "original writing rule." FED. R. EVID. 1001, *et seq.* The "original writing rule" was developed and intended to avoid inaccuracies and fraud by requiring the introduction as evidence of the original document. FED. R. EVID. 1001 (1972 advisory committee's notes). Rule 1002 still requires the production of the original document, but the very next rule provides that "[A] duplicate is admissible to the same extent as the original" provided there are no questions about its authenticity or no other reasons for requiring the original. FED. R. EVID. 1003.

Authentication of ESI

How do the rules of evidence reviewed above apply to the admissibility of ESI? In *Lorraine v. Markel American Insurance Co*, 241 F.R.D. 534 (D. Md. 2007), the court commented, "There is no form of ESI more ubiquitous than e-mail…." *Lorraine v. Markel American Insurance Co*, 241 F.R.D. at 554. In *Lorraine*, the dispute centered on whether an arbitration agreement limited the arbitrator's "authority to determine only whether the… damages [to the boat] were caused by the lightning strike or if [the arbitrator] was authorized to determine the amount of the damages as well." *Id.* at 537. The district court determined the language of the agreement was ambiguous, and extrinsic evidence could be considered by the court in determining the parties' intent. *Id.*

The parties each filed motions for summary judgment and supported their motions with various forms of documentary evidence, including e-mail communications between the attorneys. *Id.* The court found the e-mails to be relevant to the court's determination of the scope of the arbitration agreement. *Id.* at 541. However, the parties failed to authenticate the e-mails. *Id.* In other words, the parties failed to satisfy the requirement of FED. R. CIV. P. 56(e) that their motions be supported by admissible evidence. Therefore, the district court dismissed both motions without prejudice. *Id.* at 537.

Establishing the authenticity of ESI and the truth of the information contained in the files are two different matters.

The court noted the burden of authentication "is not a particularly high barrier to overcome." *Id.* at 542. It requires only a prima facie showing that the evidence is what its proponent claims. *Id.* E-mail can be authenticated by a person with personal knowledge (FED. R. EVID. 901(b)(1)), comparison with an authenticated exemplar or by expert testimony (FED. R. EVID. 901(b)(3)), the e-mail's distinctive characteristics, such as content or internal patterns (FED. R. EVID. 901(b)(4)), or establishing it is a self-authenticating business record (FED. R. EVID. 902(11)). *Id.* at 554–55.

In *United States v. Siddiqui*, 235 F.3d 1318 (11th Cir. 2000), the defendant was convicted of fraud, false statements to a federal agency, and obstruction of a federal investigation. *United States v. Siddiqui*, 235 F.3d at 1320. The defendant nominated himself for the National Science Foundation's Waterman Award. He submitted his nomination as if it had been made by an acquaintance, Dr. Yamada. *Id.* As if that were not enough, he fraudulently submitted a reference for himself, forging the signature of Dr. von Guten. *Id.*

When the National Science Foundation confirmed the reference with Dr. von Guten, he informed the foundation that he had not submitted the reference. *Id.* Things unraveled quickly for Dr. Siddiqui and, despite his decision to withdraw his

fraudulent nomination, he found himself on trial. *Id.* at 1320–21. Before the trial, the government deposed Dr. Yamada, in Japan, and Dr. von Guten, in Switzerland. *Id.* Dr. Yamada testified she received an e-mail asking her to "'please tell good words about me[ ]'" in the event she received a telephone call from the foundation. *Id.* at 1321. She testified she knew the e-mail was from Dr. Siddiqui because it included his e-mail address, and he signed it "Mo." He had previously told her Mo was his nickname. He had also used this nickname in previous e-mail messages. *Id.* Dr. Yamada also testified she received a second e-mail from Dr. Siddiqui asking her to tell the investigator that she had authorized him to sign her name to the nomination. *Id.* On cross-examination, Dr. Siddiqui's attorney introduced an e-mail from Dr. Yamada to Dr. Siddiqui. This e-mail used the same e-mail address as was used in the e-mails sent to Drs. Yamada and von Guten. *Id.*

The court noted the burden of authentication "is not a particularly high barrier to overcome."

Dr. von Guten testified he "received an email from what appeared to be Siddiqui's email address asking him to tell the Foundation that Siddiqui had permission to use von Guten's name." *Id.* Dr. Von Guten testified that he replied by e-mail to the same address, saying he could only tell the truth. *Id.*

It comes as no surprise that Dr. Siddiqui objected to the admission of the e-mail messages. The admission of the e-mails at trial was part of the basis for his appeal. *Id.* On appeal, the court noted the authenticity of the e-mails was supported by a number of factors: (1) the e-mail sent to Drs. Yamada and von Guten bore Dr. Siddiqui's e-mail address; (2) this e-mail address was the same as the address on the e-mail introduced by Dr. Siddiqui's attorney during the deposition; and (3) when Dr. von Guten used the "reply" function, his e-mail system automatically pulled up Dr. Siddiqui's address. *Id.* Furthermore, the content of the e-mail "show[ed] the author… to have been someone who would have known the very details of Siddiqui's conduct…" vis-à-vis the Waterman Award. *Id.* The e-mail to Dr. von Guten also contained statements that accurately described contact between Drs. Siddiqui and von Guten a few years earlier. *Id.* at 1323. In addition, Drs. Yamada and von Guten testified they received telephone calls from Dr. Siddiqui shortly after the e-mails were received making the same requests as those contained in the e-mails. Finally, the use of a nickname Dr. Siddiqui previously revealed to Drs. Yamada and von Guten sealed the authentication. *Id.* These circumstances were sufficient to establish authenticity. *Id.*

It has been argued that e-mail poses a novel set of authentication concerns. *Id.* For example, how can anyone establish that the e-mail was actually sent from the purported sender? *Id.* Anyone with the password could have accessed Dr. Siddiqui's e-mail account and sent the messages attributed to him. After all, while an e-mail message can be traced to a particular computer, it cannot be traced to the fingertips of a specific author. *See In re F.P.*, 878 A.2d 91, 95 (Pa. Super. Ct. 2005).

While legitimate, concerns about electronic evidence authenticity do not render its authentication impossible. As noted by the *Siddiqui* court, "[T]he 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." *Id.* The party opposed to admitting an e-mail exhibit is still free to put forth evidence calling its authenticity into question. A prima facie showing of authenticity is not the same as a court finding "that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury ultimately might do so." *United States v. Safavian*, 435 F. Supp. 2d 36, 38 (D.D.C. 2006). In addition, an e-mail, like any other type of document, can be deemed authentic if produced by a party during discovery, and subsequently offered by a party-opponent. *See Sklar v. Clough*, 2007 WL 2049698 at *4–5 (N.D. Ga.) (holding that e-mails produced by the defendants during discovery were deemed authentic when offered by the plaintiffs in support of their motion for summary judgment).

What about other forms of electronic communication, such as chat room logs? A chat room is a site on the Internet where a number of users communicate in real time, usually dedicated to one topic, which can range from the benign and possibly helpful to the most vile and repulsive.

In *United States v. Tank*, 200 F.3d 627 (9th Cir. 2000), the defendant. Mr. Tank, was convicted of various child pornography-related offenses. He belonged to an Internet chat room devoted to child pornography. *Id.* at 629. One of the defendant's fellow chat room members, Mr. Riva, saved all online chat room conversations on his computer. *Id.* Before any investigation into this sordid group began, Mr. Riva deleted any nonsexual conversations and the date and time stamps from his text files to decrease the size of the saved files. *Id.* When Mr. Riva was arrested on child molestation charges, law enforcement officials discovered these edited conversation files on his computer. *Id.*

Finding Mr. Riva's conversation files resulted in the arrest and eventual prosecution of Mr. Tank. *Id.* Mr. Tank objected to the admission of the chat room logs because they were incomplete and Mr. Riva might have made undetectable changes to the substance of the conversations or in the names used in the correspondence. *Id.* at 630. In authenticating the chat room logs, the government presented testimony from Mr. Riva describing how he prepared the logs and that the exhibits accurately represented the conversations. *Id.*

In addition, the screen name "Cessna" appeared throughout the conversations. The authenticating evidence presented by the government established that Mr. Tank used the screen name "Cessna" when he participated in the chat room conversations. *Id.* Other chat participants testified that when they arranged to meet "Cessna," it was the defendant who appeared for the meeting. *Id.* at 630–31. Therefore, the court held that the government met its prima facie showing of authentication. Mr. Tank's argument about the potential incompleteness of the conversations was relevant to the weight of the evidence, not its admissibility. The government's responsibility was to present proof that the logs were com-

plete and the substance was unaltered. The defendant was free to counter the government's proof with evidence to establish the logs had been altered.

When authenticating chat room conversations or instant messages, it's critical to establish the author's identity—the identity of the actual person behind the screen name pseudonym. Establishing author identity can be achieved by offering testimony of someone who knows the party and his or her screen name. Just as we saw with Dr. Siddiqui's e-mail, if content is peculiar to a particular person, content of messages can be used to connect the messages to that person and to establish authorship.

The way characteristics of a particular person's e-mails can be used is highlighted in *People v. Pierre*, 838 N.Y.S.2d 546 (App. Div. 1st Dept. 2007), a case in which the defendant was convicted of murdering his girlfriend because she refused to have an abortion. *Id*. at 548. Mr. Pierre's undoing was instant messaging. *Id*. at 548–49. One witness, a friend of the defendant and his accomplice, testified as to his personal knowledge of Mr. Pierre's screen name. *Id*. The deceased's cousin testified she sent an instant message to that particular screen name and received a reply that would have made no sense unless the reply had been sent by Mr. Pierre. *Id*. at 549. The court found the message constituted an admission of the defendant and permitted testimony as to the message's content even though the witness had neither printed the message nor saved it. *Id*. at 548–49.

The failure to present evidence identifying the e-mail's author can be fatal to authentication. For example, in *People v. Von Gunten*, 2002 WL 501612 (Cal. Ct. App.), the defendant was charged with assault with a deadly weapon. *Id*. at *1. The defendant claimed an individual named Beever committed the assault. He attempted to introduce a "cut and pasted" transcript of a series of instant messages between a friend and an individual using the screen name BuckaRoo 20. *Id*. at **4–5. The defendant's friend testified she knew at one time Beever used BuckaRoo 20 as his screen name. The evidence also established that anyone with the correct password could send messages under the screen name BuckaRoo 20. Software that would allow a third party to decode a particular screen name's password was also discussed. The conversations' transcript did not contain the subject header, date, or time at which the instant messages. Therefore, because of the slim evidence connecting the screen name to the individual, Beever, the court refused to admit the transcript as evidence. *Id*. at *5.

Today, it is the exception rather than the norm, to find a business or governmental agency without a website. Organizations, clubs, and individuals have websites. Often, the information that is posted on a website can prove useful in the litigation of your case. Some courts, however, are very skeptical of the trustworthiness of information found on the Internet. In *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, 76 F. Supp. 2d 773 (S.D. Tex. 1999), the court was less than impressed with the information from the Internet.

In *St. Clair*, the plaintiff filed suit for injuries he received while working aboard a boat he claimed was owned by the defendant. *Id*. at 774. The defendant filed a motion to dismiss, contending it did not own the boat. *Id*. The plaintiff responded with "'evidence'—taken off the Worldwide Web…—revealing that Defendant…'" owned the boat. *Id*. The "evidence" was from the United States Coast Guard's on-line vessel database. *Id*. In rejecting the evidence, the court noted that it viewed the Internet "as one large catalyst for rumor, innuendo, and misinformation." *Id*. The court rejected the ownership evidence because the plaintiff had failed to "overcome the presumption that the information discovered on the Internet is inherently untrustworthy." *Id*. The presumption could have been overcome with evidence authenticating the information as having come from the website and having been posted to the site by the Coast Guard. *Id*. at 775. Without such evidence, the court rejected the "voodoo information" from the Internet. *Id*. The *St. Clair* court's colorful comments about Internet information's untrustworthiness recognized, as have other courts, that "information on [the] internet… presents special problems of authentication." *Terbush v. United States*, 2005 WL 3325954 at *5 n. 4 (E.D. Cal.).

Can the presumption of the untrustworthiness of information on the Internet be overcome if a witness testifies that he or she went to a particular website, viewed its information, printed it, and the printout accurately represents what he or she viewed? The answer varies, depending on the court. Some courts require verifying testimony from an employee of the website's owner to overcome concerns that a hacker may have put the information on the website. An example of a case in which a court believed a hacker might have authored and posted particular website information is found in *United States v. Jackson*, 208 F.3d 633 (7th Cir. 2000).

In *Jackson*, the defendant, Ms. Jackson, apparently had packages sent to her address via United Parcel Service. The packages contained artwork depicting African American culture. Evidence established that the packages arrived at her address, and when they did, they were undamaged. The defendant, however, claimed that not all of the packages arrived, and those packages that did arrive were damaged and contained racial epithets. *Id*. at 634–35. She filed a claim with UPS for $572,000, although she only paid $2,000 for the artwork. *Id*. at 635. UPS denied the claim. The defendant alleged that UPS denied the claim because of racist elements within the company. *Id*. In addition, the evidence showed that she also sent letters containing racially charged language to various prominent African Americans via UPS. *Id*. The letters showed return addresses to various white supremacist organizations. *Id*.

During her trial for, among other things, wire fraud, Ms. Jackson sought to introduce web postings from the websites of the white supremacist organizations which purportedly showed these organizations took credit for the racist mailings. *Id*. at 637. The court sustained the government's objection for various reasons, one of which was a lack of authentication. The court concluded that the defendant failed to show that the web postings were posted to the website by the groups, rather than "being slipped onto the groups' websites by [the defendant]…, who was a skilled computer user." *Id*. at 638. In other words, the defendant had not produced evidence to overcome the presumption of the untrustworthiness of information on the Internet.

Some courts allow admission of web postings or printouts without testimony from the owner of the website. These courts tend to view FED. R. EVID. 901(a)'s require-

ments as more elastic than courts that require verifying testimony about the origins of a website's information. In *United States v. Standring*, 2006 WL 689116 (S.D. Ohio), the court accepted printouts from various websites based upon a witness' declaration that he visited various websites, accessed the information, and printed the information. The printouts contained the dates on which the websites were accessed and the web addresses of the various sites. Perhaps this additional information gave the court a level of comfort it might not otherwise have found in the witness's declaration alone.

An e-mail, like any other type of document, can be deemed authentic if produced by a party during discovery, and subsequently offered by a party-opponent.

On the other hand, some courts have been willing to accept electronic documents as evidence based upon the affidavits of witnesses who retrieved them. For example, in *Kassouf v. White*, 2000 WL 235770 (Ohio App.) the plaintiff filed a defamation action against Cleveland, Ohio's mayor because the mayor, in opposition to the plaintiff's proposed construction of a hotel, referred to the hotel as a "$39.95 flophouse." In support of his motion for summary judgment, the mayor submitted documents from the hotel chain's website showing rooms in the Cleveland area rented for anywhere from $35 per night to $119 per night. The documents, which were accepted by the court, were authenticated by an individual's affidavit that he accessed the chain's website, retrieved the attached documents, and the documents accurately reflected information on the website. *See also, Moose Creek, Inc. v. Abercrombie & Fitch*, 331 F. Supp. 2d 1214, 1225 n.4 (C.D. Cal.), *aff'd*, 114 Fed. Appx. 921 (9th Cir. 2004); *Johnson-Wooldridge v. Wooldridge* 2001 WL 838986 at *4–5 (Ohio Ct. App.).

Printouts from private websites are not self-authenticating; therefore, testimony from a witness knowledgeable about the website is required. *See In re Homestore.com Securities Litigation*, 347 F. Supp. 2d 769 (C.D. Cal. 2004). Printouts from government websites, however, can be self-authenticating. Rule 902(5) provides that "[b]ooks, pamphlets, or other publications purporting to be issued by public authority[ ]" are self-authenticating. FED. R. EVID. 902(5). In determining whether Rule 902(5) applies to documents from government websites, courts have applied the plain meaning to the terms "books, pamphlets, or other publications" and concluded the rule does cover such documents. *See United States v. Premera Blue Cross* 2006 WL 2841998 at *3–4 (W.D. Wash.).

Unless you know your judge and his or her authenticity standard, it is best to depose the webmaster or another sufficiently knowledgeable employee to establish the website evidence's authenticity. If you are unable to secure this testimony, include the URL address (*i.e.*, the www._____) on the printout, the date on the printout, and any other evidence distinctive to the website to establish its authenticity.

Business records maintained in an electronic format also require authentication. The language in both Rule 902(11) for authentication and Rule 803(6) about an exception to the rule against hearsay, is very similar. Therefore, the authenticity analysis and the business record exception analysis are merged into one inquiry. *See In re Vee Vinhee*, 336 B.R. 437, 444 (9th Cir. BAP 2005). As we have seen, the authentication standards vary by court. With respect to electronic business records, some courts have adopted Professor Imwinkelreid's 11-step process:

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.

In re Vee Vinhee, 336 B.R. 437, 444 (quoting Imwinkelreid, Evidentiary Foundations §4.03[2] (5th ed. 2005)). As noted in *In re Vee Vinhee*, "The 'built-in safeguards to ensure accuracy and identify errors' in the fourth step subsume details regarding computer policy and system control procedures, including control of access to the database, control of access to the program, recording and logging changes, backup practices, and audit procedures to assure the continuing integrity of the records." *In re Vee Vinhee*, 336 B.R. at 446–47.

In *In re Vee Vinhee*, the court found the testimony of the records custodian was lacking. His testimony failed to establish "his job title or anything about his training or experience…." *Id.* at 448. Furthermore, his testimony revealed that he did not know the type of computer used by American Express, nor did he know the type of software used. The court found the testimony to be too general and conclusory to authenticate the electronic records. *Id.* at 447 n. 9 and n. 10.

Other courts, however, have been more lenient in authenticity rulings. These courts have generally required only the testimony of a witness familiar with the record-keeping system who was able to verify that the retrieved records were produced from the electronic information generated contemporaneously with the transaction at issue. *See Sea-Land Serv., Inc., v. Lozen Int'l.*, 285 F.3d 808 (9th Cir. 2002); *United States v. Meienberg*, 263 F.3d 1177 (10th Cir. 2001). As with everything involving litigation, you must know your audience. If you err, err on the side of providing the court with more information than needed for authentication rather than less.

Sometimes, no matter how prepared you are, things go wrong. A witness changes his or her testimony. Your client suddenly becomes the worst possible witness. A potential juror was not forthcoming during *voir dire*. But authentication is a different kind of a problem. If your exhibit is rejected because it lacks authentication, you probably have only yourself to blame. Thoughtful, advance preparation can avoid such a painful and embarrassing moment.

Preparation should start during discovery. During discovery, ask questions designed to aid authentication later. For example, does the opposing party have an e-mail address, if so what is it, and how long has he or she used it? Ask questions about the opposing party's prior e-mail addresses and who has access to the various e-mail accounts, both active and inactive. Ask about the screen names he or she uses and what the names mean. Has he or she ever had a problem with others accessing his or her accounts and sending messages attributed to him or her? Does he or she have a website, and if so, who is the webmaster, and who controls the content of the website? If he or she can make some website changes, find out what types he or she is authorized to make. Find out what types of website changes his or her employees are authorized to make. Does he or she maintain a blog or have a MySpace account? If so, find out as much information as you can about it. All of the information mentioned above can be very useful later when you are trying to authenticate evidence.

Hearsay

Once the authentication requirement has been satisfied, you have to address the rule against hearsay. If a statement is offered for its truth and the real witness, or declarant, is not in the witness chair, you must either establish that it is nonhearsay, or fits a hearsay exception.

A statement is not hearsay if it is an admission by a party-opponent. The statement must be "offered against a party and is… the party's own statement, in either an individual or representative capacity." Fed. R. Evid. 801(d) (2)(A). Remember our friend Dr. Siddiqui? Some of the e-mails at issue in his case were written by him, and as such, could be offered as an admission by Dr. Siddiqui to establish truth that worked against him.

This rule—that a party's own admission in an e-mail can be offered as a statement—generally holds, unless the party can establish the e-mail was sent as the result of a computer malfunction. In *Ermolaou v. Flipside*, 2004 WL 503758 (S.D.N.Y.), the plaintiff entered an Internet lottery game in which she picked numbers for the one million dollar, ten million dollar, and twenty million dollar games. She received two e-mails from the operator of the lottery. The first e-mail provided her with the winning numbers in each game, and to her surprise, she matched every number in each game. Sadly, the second e-mail notified her that the first e-mail had been sent in error and provided her with the actual winning numbers, none of which she matched. The plaintiff sued the operator of the lottery and argued that the first e-mail constituted an admission of the defendant. The court rejected her argument because the evidence established the first e-mail was sent as the result of a computer error. Therefore, it did not constitute an admission.

A second rule is that the "statement offered against a party… is… a statement of which the party has manifested an adoption or belief in its truth…" Fed. R. Evid. 801(d)(2)(B). In the world of electronic mail, merely forwarding an e-mail to another recipient may be enough to make a statement contained in it an adoptive admission. In *Sea-Land Serv., Inc., v. Lozen Int'l*, the employee sent an e-mail to a second employee and the latter forwarded the e-mail to the defendant and included her own comments, which manifested her own belief in the statements made by the e-mail originator in the original e-mail. The court found the act of forwarding an e-mail with comments indicating agreement with beliefs expressed by the e-mail chain originator, constituted an adoptive admission under Fed. R. Evid. 801(d)(2)(B). *Sea-Land Serv., Inc., v. Lozen Int'l*, 285 F.3d at 821. Similarly, if the evidence shows that the e-mail was written by "a person authorized by the party to make a statement concerning the subject, or… a statement by the party's agent or servant concerning a matter within the scope of the agency or employment, made during the existence of the relationship[ ][,]" then the e-mail qualifies as nonhearsay. Fed. R. Evid. 801(d)(2)(C)–(D). In *Perfect 10, Inc. v. Cybernet Ventures, Inc*, 213 F. Supp. 2d 1146, 1155 (C.D. Cal. 2002), the court addressed whether e-mail messages sent by Cybernet's employees were nonhearsay under Rule 801(d)(2)(D). Because the messages were sent by employees, concerned matters within the scope of their employment, and were prepared during the existence of the employment relationship the court held the messages were nonhearsay.

E-mail, however, can also satisfy one or more of the 23 exceptions to the rule against hearsay. For example, if the HR director for your client sent an e-mail to her superior detailing an interview with an employee making a sexual harassment complaint, the e-mail might be admissible in subsequent litigation. Under Rule 803(1), provided the e-mail was prepared during the conversation, or very shortly thereafter, it could be admitted into evidence as a present sense impression. *See United States v. Ferber*, 966 F. Supp. 90, 98–99 (D. Mass. 1997).

Some courts…
are very skeptical of the trustworthiness of information found on the Internet.

Could the e-mail also be admitted under the business records exception? Perhaps, but not every document made in a business setting falls within the business records exception. The critical questions to be answered are whether the business routinely required the HR director to report to her supervisor and hence whether she had a business duty to report these matters. Without affirmative answers to these questions, the e-mail would not be admissible under 803(6).

The various exceptions should be examined in detail, in light of the facts of your case and the circumstances of the e-mail, to determine if they apply. For example, a text message sent from a witness to an accident might fit the excited utterance exception.

Often when e-mail is received it has been forwarded by various recipients, each of whom may add his or her own comments to the original. Each message in this e-mail

chain must be analyzed and found to fit within an exception. In *Rambus Inc. v. Infineon Tech. AG*, 348 F. Supp. 2d 698 (E.D. Va. 2004), the court held that for an e-mail chain to be admissible under the business records exception, the proponent of the e-mail must show that each declarant was acting in the course of regularly conducted business. Of course, it might be possible to fit each part of the chain within other exceptions.

The rules against hearsay and its exceptions apply to websites as well. If a website belongs to a party-opponent, the information taken from the website can be considered an admission. If the information is hearsay, it can fit one or more of the exceptions. A printout from a website, such as Kelley Blue Book, is admissible under FED. R. EVID. 803(17) to establish the value of a car. In *Neloms v. Empire Fire & Marine Ins. Co.*, 859 So. 2d 225, 232 (La. Ct. App. 2003), the plaintiff submitted a printout from the website to establish the value of her car. The court held that the printout was admissible because these types of publications are widely relied upon to determine the values of cars.

Original Writing Rule

If you must "prove the content of a writing, recording, or photograph, the original… is required, except as otherwise provided…" in the rules of evidence. FED. R. EVID. 1002. In other words, if you are not proving the veracity of the content of the writing, recording, or photograph, this rule does not apply. For example, if you called a witness to testify in a car wreck case as to what the plaintiff's car looked like following the wreck, and you used a photograph as part of the testimony, the rule would not apply. *See* FED. R. EVID. 1002 (1972 advisory committee's notes). The rule would apply in a medical malpractice case to X-rays or MRI images. *Id.*

The rules provide that a printout of data stored in a computer or similar device is an "original" provided it accurately reflects the data. FED. R. EVID. 1001(3). For this reason, in *Laughner v. State*, 769 N.E.2d 1147 (Ind. Ct. App. 2002), the court permitted a police officer to present a "cut and pasted" version of his text messages with the defendant. The officer "cut and pasted" the text of the conversations from the chat room into a word processing program and printed the document from the word processing program. The court concluded that based upon 1001(3) the printout was an original.

When the rule applies, however, you need not produce the original if a duplicate is available. FED. R. EVID. 1003. If, however, the authenticity of the original is genuinely questionable, or doubts exist about the reliability of the method used to make the duplicate, the duplicate cannot be used.

Can evidence other than an original or duplicate be used to prove the veracity of the content of the writing, recording, or photograph? Yes, provided the original or duplicate is lost or destroyed, not obtainable, or is in the possession of the opponent. FED. R. EVID. 1004. An example of a case in which a duplicate sufficed to prove content accuracy, can be seen in *King v. Kirkland's Stores, Inc.*, 2006 WL 2239203 (M.D. Ala.). In *King*, the plaintiffs sued the defendant alleging they were fired because of their race. One of the plaintiffs was permitted to testify as to the contents of an e-mail from a customer complaining the defendant employed too many African Americans at the store where the plaintiffs worked. The plaintiff claims she saw the e-mail when it was forwarded to the store. According to the plaintiffs, they were terminated shortly after the e-mail was forwarded to the store's management. The court held that because the e-mail was allegedly in the possession of the defendant, the plaintiff could testify as to its contents.

Conclusion

The role that electronic evidence plays will vary from case to case. But with camera phones, PDAs, laptops, traffic cameras, websites, and chat rooms, our chance of having to deal with electronic evidence continues to increase. Not only must we learn what to look for and what questions to ask during discovery, but we must learn how to use the evidence to our advantage.

The applicable standards regarding the authenticity and admissibility of evidence can vary from court to court. This is particularly true with electronic evidence, given the doubts some courts hold regarding its reliability in certain forms. Therefore, "[u]nless [you] know what level of scrutiny will be required, it would be prudent to analyze electronic [evidence] that [is] essential to [your] case by the most demanding standard." *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534, 574 (D. Md. 2007). Failure to prepare for the most demanding standard may cost you the benefit of the electronic evidence you diligently collected during the pretrial phase of your case.