THE JOURNAL OF THE TRIAL EVIDENCE COMMITTEE

proof

SECTION OF LITIGATION | AMERICAN BAR ASSOCIATION
SUMMER 2010 VOL.18 NO.4

The Reliability, Admissibility, and Power of Electronic Evidence

By Zachary G. Newman and Anthony Ellis

It is impossible to ignore that electronic communication has become the predominant and preferred form of communication in all aspects of business and social interaction. Negotiations, settlement discussions, confidential communications, transaction closings, and the completion of contracts for goods or services are all accomplished through email, BlackBerry Messenger, Bloomberg Messenger, and even text messages. With the rapidly increasing popularity of social, business, and personal networking forums, it seems clear that this evolution in the way that we communicate as a society is only going to continue and expand. Yet, despite the fact that electronic data is permanent, nearly indestructible, and easily transferrable, the public at large continues to view email and other electronic communications with an air of informality that was rarely associated with traditional professional letters or memoranda. Nowhere is this more obvious

Continued on page 10

in this issue

ABA Section of Litigation
AMERICAN BAR ASSOCIATION

Electronic Evidence

Continued from page 1

than the avalanche of data incriminating golfer Tiger Woods. Rumors are one thing, but show the public text messages and it instantly becomes incontrovertible.

For litigators, the advent of electronic data has been both a blessing and a curse. The headaches associated with electronic discovery have been well-documented, and this article will not delve into them again. Suffice it to say that it is not uncommon even in smaller trials to have over a terabyte of data and many thousands of documents to review and produce. Electronic data simply provides a treasure trove of information in every case of every size that can ultimately prove, disprove, or color litigation. Moreover, contemporaneous electronic communications seem to have an air of reliability that is not generally credited to someone's recollection of events, particularly if those events occurred years before the matter ultimately comes to trial.

While we as attorneys have been learning to deal with such concepts as electronic discovery, metadata, email retrieval, and spoliation, litigation lawyers need to remember the basics of evidentiary procedure. Courts are not relaxing evidentiary rules simply because the world has become incredibly informal in terms of communication and interaction. Accordingly, this article focuses on establishing the authenticity of electronic evidence; provides a primer on dealing with hearsay in the context of electronic documents, which is a core evidentiary consideration inherent in electronic communication; and discusses noteworthy cases involving electronic discovery.

Zachary G. Newman

Anthony Ellis

Zachary G. Newman is a partner and Anthony Ellis is an associate of Hahn & Hessen LLP in New York, New York. Phil Lem, a first-year associate at the firm, contributed to the article and undertook the arduous task of assembling and analyzing the research.

Reliability and Authentication

Suppose you are representing a client who claims its contractual relationship with one of its largest customers was tortiously interfered with by a competitor. Given your appreciation of the importance of electronic data, you requested all text messages, instant message communications, and, of course, emails. In the documents produced, you find a series of text messages clearly establishing that your client's competitor knew of your client's contract and maliciously convinced your client's customer to breach his contract. Although this appears to be fantastic evidence, it is useless unless you can find a way to introduce it into the litigation.

To do so, you must first establish that the evidence is reliable and authentic. Authentication is the basic process of proving evidence is in fact genuine. The process by which you will have to determine the authenticity, reliability, and admissibility of evidence must start immediately as opposed to the eve of trial. Too often, counsel appear at pretrial conferences without any clue, let alone a plan, for authenticating and admitting documents into evidence during trial. Litigators need to concern themselves with authenticity and admissibility from day one to successfully manage discovery and conduct a successful lawsuit.

Although there appears to be a public presumption that emails and texts are credible, the fact is that electronic data can be manipulated, re-created, or corrupted with ease. Thus, litigators need to critically analyze the reliability and authenticity of the materials before such materials ever come before the finder of fact, whether a judge or jury, and must pay attention to and address the authentication prerequisites contained in the evidentiary rules.

Given the costs associated with authenticating electronic documents, it is becoming increasingly standard and recommended to obtain an agreement with opposing counsel prior to trial that electronic documents produced by the adverse party or reliable sources be authentic. However, to the extent that no such agreement exists, the relevant federal or state rules will likely outline the methods by which evidence can be authenticated.

In the federal court system, Federal Rules of Evidence (FRE) 901 and 902 govern authentication. FRE 901(a) notes that evidence is authenticated if there is "evidence sufficient to support a finding that the matter in question is what its proponent claims." FRE 901(b) then provides a list of potential ways that a litigant can satisfy this standard. For example, the easiest way to authenticate the data is under FRE 901(b)(1), which allows a witness with personal knowledge to authenticate that the data is what it is claimed to be. One simple way to comply with this standard is to introduce the electronic document during a deposition and have the creator or recipient of the email confirm that the email is genuine.

If such testimony is unavailable, courts have permitted electronic data to be admitted under FRE 901(b)(4), which permits authentication through distinctive characteristics such as the document's "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." In *United States v. Safavian*, the court admitted emails based on the email addresses contained in the "to" and "from" fields, and because other identifiable matters such as the work involved, signatures, and other personal and professional references.[1] The court permitted other emails to be authenticated under FRE 901(b)(3) by allowing the comparison of email addresses and formats to permit related emails into evidence.

Under FRE 902(7), business emails can be self-authenticating with information showing the origin of the transmission or other identifying

marks. This can be done through the authentication of company logos, email addresses, and other corporate identifiers. One trial court found emails to be authenticated when accompanied with a declaration that the emails were retrieved from the company's computers and the printouts were accurate representations of the retrieved messages.[2]

Information necessary to establish that the document is a business record can be obtained during a deposition. For example, ask the deponent if he or she recognizes the format of the email, or if the email looks the same as if he or she printed out an email in his or her office. Ask the deponent if he or she is familiar with the email addresses, or the domain names contained in the email. Determine if the document was printed out from the deponent's computer system, and authenticate printouts by securing testimony that the deponent believes the information is reliable because it is the same information that is available through the deponent's assigned work computer.

Finally, in certain cases, courts have held that electronic data can simply be authenticated by confirming that they were produced by the adversary during document discovery, as the act of production implicitly authenticates the documents.[3]

Of note, the mere fact that electronic data can be manipulated is not a substitute for hard evidence that the documents were manipulated or immediate grounds for preclusion. As the *Safavian* court noted:

> The *possibility* of alteration does not and cannot be the basis for excluding e-mails as unidentified or unauthenticated as a matter of course, any more than it can be the rationale for excluding paper documents (and copies of those documents). We 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. The defendant is free to raise this issue with the jury and put on evidence that e-mails are capable of being altered before they are passed on. Absent specific evidence showing alteration, however, the Court will not exclude any embedded e-mails because of the mere possibility that it can be done.[4]

Admissibility of Electronic Data and the Hearsay Rule

Even if you can establish that electronic data are authentic, you are only halfway there. As with all evidence, you also must establish that the documents are admissible under the law. This section focuses on overcoming hearsay objections. Electronic data that is offered for the truth of the matter asserted is classic hearsay and thus generally inadmissible under evidentiary rules. To admit the emails as direct evidence, the proponent needs to satisfy an exception to the hearsay rule.

As with other documentary evidence, it is important to focus on who prepared and transmitted the electronic communication. For example, the argument for admissibility against a company is solidified if the email preparer is an officer or employer of that company.[5] Emails sent by corporate officers or employees may be considered admissions by a party's agent under FRE 801(d)(2)(D) and therefore fall outside the definition of hearsay.

Assuming that the document was not prepared by the opposing party, the vast majority of corporate email is generally introduced into evidence under the business-records exception to the hearsay rule. "A party seeking to introduce an email made by an employee about a business matter under the hearsay exception under FRE 803(6) must show that the employer imposed a business duty to make and maintain such a record."[6] 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."[7] Emails are admissible business records when they are timely recorded, regular activities, they memorialize events and conditions, and they have no indicia of untrustworthiness.[8]

Although this standard may seem to be easily satisfied, counsel should be aware that courts have sometimes adopted a rigid approach to the business-records exception. For example, in *United States v. Ferber*, the court found that emails submitted by the government did not fall under the business-records exception because "while it may have been [an employee's] routine business practice to make such records, there was no sufficient evidence that [the employer] required such records to be maintained."[9] If the proponent fails to submit information regarding the practice or composition of the emails at issue, a court likely will deem them inadmissible as business records.[10]

In addition, counsel should carefully prepare deposition witnesses for examination on this issue. In one case, the court rejected the emails at issue because the email sender testified at deposition that (a) she did not know where she got the information she included in the email about missed shipments, (b) she did know what she was referring to when she made certain statements about vendor charges, and (c) she did not know what she meant when she said that there were missed shipments.[11] The court found that the plaintiff failed to present evidence that the email sender either made or recorded her statement based on personal knowledge of the issues of discontinued business, missed shipments, or vendor-compliance charges. Therefore, the court granted the defendant's motion to strike the email as inadmissible hearsay.

Furthermore, given the amount of information contained in a single email chain, one has to be aware of multiple levels of hearsay. Courts frequently reject email discovery when the proponent is unable to satisfy hearsay exceptions for each account contained in an email.[12] This concern is particularly apparent when dealing with long email chains, which may result in numerous hearsay and admissibility issues. For example, where there is no evidence that the emailing party had firsthand knowledge of the matters contained in the email but rather was forwarding someone else's version, courts are more likely to preclude the entire email from being admitted.[13]

Emails forwarded by a party can be used to demonstrate his or her adoption of its content.

Litigants also should be aware that the admission of email evidence does not necessarily provide a clear path for email attachments. Information contained in or attached to emails, such as sales records, are potentially subject to independent scrutiny under the evidentiary rules. Attachments will be admissible under the business-records hearsay exception when the underlying data is regularly received by email and the emails were retained as records of each order.[14]

Admissions and Hearsay Exceptions

Even if the electronic data is hearsay, emails and texts can be admitted into evidence on other grounds or under one of the standard hearsay exceptions. For example, the proponent may not offer the evidence for the truth of the matter asserted therein but rather to prove that certain meetings or events happened or that certain strategies were employed, as they are not offered to prove the truth of the matters asserted within them but as circumstantial evidence of events or occurrences.

Electronic communications can also be offered against a party as party admissions, rather than as hearsay. When "it is the party's own statement, either in individual or representative capacity," the evidentiary rules take that statement outside the definition of hearsay when it is offered into evidence by the adverse party.[15] Thus, when the proffering party lays a foundation to show that an adversary's email relates to a matter within the scope of the sender's employment, emails sent from his corporate email address likely will be deemed admissions against the employer under FRE 801(d)(2).

Emails also could be admitted as admissions by coconspirators in furtherance of a conspiracy claim.[16] The proponent must show that (a) there was a conspiracy, (b) the declarant and the party against whom the statement is offered were members of the conspiracy, and (c) the statements were made in furtherance of the conspiracy.[17] The prerequisites for admissibility are considered a preliminary question under FRE 104(a), and are therefore resolved by the court, not the jury.[18] Though the court may consider the content, "for such statements to be admissible, there must be some independent corroborating evidence of the defendant's participation in the conspiracy."[19]

An email made by someone else can be attributed directly to a party as an admission under FRE 801(d)(2)(A). The context and content of certain emails can demonstrate that the party "manifested an adoption or belief" in the truth of the statements of other people as he or she forwarded their emails.[20] Emails forwarded by a party, therefore, can be used to demonstrate his or her adoption of its content, and can be admitted as an adoptive admission under FRE 801(d)(2)(B).[21]

In addition, there are a number of exceptions to the hearsay rule. For example, under FRE 803(3), a statement is not excluded by the hearsay rule if the statement is of the declarant's then-existing state of mind, emotion, sensation, or physical condition (such as intent, plan, motive, design, mental feeling, pain, and bodily health), but not including a statement of memory or belief to prove the fact remembered or believed unless it relates to the execution, revocation, identification, or terms of the declarant's will. There is ample authority for the application of these hearsay exceptions, and it is important to analyze each part of the email communication to determine whether a portion of it may be admissible and useful in the event the entire communication is inadmissible. For example, some courts permit a victim's statements about being afraid of the accused to establish a state of mind but may require the redaction of why the victim was afraid.[22]

Another approach when faced with otherwise inadmissible electronic data is to offer the information to prove motive, intent, or beliefs, as opposed to proving the truth of the matter asserted. For example, in one sex-discrimination case, the court found that emails referring to a client as an "idiot" and suggesting he be shot were not hearsay as they were not being used to prove the statements were true, but rather were being used to show that the company acted reasonably in firing the employee.[23]

The Power of Email and Electronic Data

The impact of the emails can have a long-lasting effect on the court or jurors, regardless of the reason for being admitted into evidence and notwithstanding any related jury instructions as to the limitations of that evidence. The powerful impact that emails can have on a party's theory of the case is well demonstrated in *United States v. Safavian*, which also provides an excellent tutorial on how to authenticate and admit emails

into evidence.[24] That case involved the political-corruption prosecution of the General Services Administration's deputy chief of staff. The email evidence—which consisted of over 250 emails—was critical to the case. The government sought a pretrial ruling as to the admissibility of the emails and its intent to have an FBI agent read the emails into evidence before the jury.

The court admitted the majority of the emails as they explained the deputy chief of staff's motive and intent at the time "he undertook certain actions or, arguably, when he made his representations during the investigations by the GSA's Office of Inspector General and the Senate Committee on Indian Affairs." The jury was to be instructed that the emails could only be considered insofar as they have had some impact on the deputy's "state of mind or provided him with a motive to make false statements or obstruct justice."

Email evidence has quickly become the driving force behind many court decisions. For instance, in *Demarco v. Lehman Brothers Inc.*, the court denied a motion to dismiss alleged securities violations brought in a class action claiming Lehman Brothers fraudulently induced them with inflated ratings and recommendations to buy stock.[25] The internal emails revealed serious concerns over the stock, which flatly contradicted the "buy" rating Lehman Brothers assigned to the stock. These emails, the substance of which was spread throughout the complaint, helped the class-action plaintiffs defeat the motion to dismiss, and immediately educated the court as to the alleged misleading stock rating.

In *Jamsports & Entertainment, LLC v. Paradama Products*, the court denied summary judgment where the email evidence was considered strong evidence of an intent to engage in anticompetitive behavior as alleged in the lawsuit.[26] Emails from the president of the division reflected his attempts to gain exclusivity over sports venues, supporting the plaintiff's claims. In one email, the president said he needed to "lock up" key stadiums and, in another email, he stated he had "made crystal clear" to a venue that if it allowed a competitor access, the venue "may be forcing [him] to look elsewhere."

In *SEC v. Mozilo*, the court found that certain emails supported a finding that the defendants acted with the intent to deceive or defraud.[27] Despite public pronouncements as to the viability and stability of their company's mortgage products, executives' internal and private emails expressed concern over the value of mortgages. In one email, Mozilo admitted that "it is just a matter of time that we will be faced with much higher resets and therefore much higher delinquencies." In another email, Mozilo informed another defendant that he was aware that borrowers were lying about their income in the application process. In yet another email, Mozilo wrote that "[w]e have no way with reasonable certainty, to assess the real risk of holding these loans on our balance sheet." On the basis of these emails, the court refused to find that Mozilo's statement that "[w]e believe we have prudently underwritten" the subject loans was neither false nor misleading.

The case of *Pursuit Partners, LLC v. UBS AG* demonstrates the danger of informal "stream of consciousness" email writing.[28] Defending claims of securities fraud and fraudulent concealment in connection with its sale of collateralized debt obligations (CDOs) from the bank, UBS understandably had difficulty in credibly explaining away emails in which one UBS employee named as a defendant in the action emailed a colleague and stated he had "sold more crap to Pursuit." In another email, a UBS employee sent an email to a UBS director referring to a CDO in their inventory as "vomit." Not surprisingly, based on these emails, the court held that the plaintiffs met their burden of satisfying the probable-cause standard on the issue of whether UBS had superior knowledge that was not readily available to Pursuit.

Conclusion

Email evidence is becoming more and more prevalent in lawsuits. Therefore, significant time should be devoted to identifying and analyzing the authentication and admissibility issues relative to the electronic data involved in the litigation. Addressing these issues at the earliest possible phase is critical to a successful evidentiary presentation on summary judgment, at a hearing, or at trial.

The groundwork for establishing authenticity and admissibility should begin as soon as the information is gathered and reviewed, as additional discovery may be required to ensure that the electronic evidence can be used in court.

Endnotes

1. United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006), *rev'd on other grounds*, 528 F.3d 957 (D.C. Cir. 2008).
2. Scheuplein v. City of W. Covina, 2009 Cal. App. Unpub. LEXIS 7805, at*26–27 (Cal. Ct. App. Sept. 29, 2009).
3. Schaghticoke Tribal Nation v. Kempthorne, 587 F. Supp. 2d 389, 397 (D.Conn. 2008); John Paul Mitchell Sys. v. Quality King Distribs., Inc., 106 F. Supp. 2d 462, 472 (S.D.N.Y. 2000).
4. *Safavian*, 435 F. Supp. 2d 36 at 41 (emphasis in original).
5. Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 454 F. Supp. 2d 966, 974 (C.D. Cal. 2006).
6. Canatxx Gas Storage Ltd. v. Silverhawk Capital Partners, LLC, Civ. No. H-06-11330, 2008 U.S. Dist. LEXIS 37803, at *36–37 (S.D. Tex. May 8, 2008).
7. United States v. Ferber, 966 F. Supp. 90, 98 (D. Mass. 1997).
8. Phillip M. Adams & Assocs., LLC v. Dell, Inc., 621 F. Supp. 2d 1173, 1186 (D. Utah 2009).
9. *Ferber*, 966 F. Supp. at 98.
10. New York v. Microsoft, No. CIV A. 98-1233 (CKK), 2002 U.S. Dist. LEXIS 7683, at *9 (D.D.C. Apr. 12, 2002) (declining to admit emails under the business-records hearsay exception because there was a "complete lack of information

regarding the practice of composition and maintenance of" the emails).

11. Age Group Ltd. v. Regal West Corp, No C07-1303BHS, U.S. Dist. LEXIS 92924, at *7–8 (W.D. Wash. Nov. 14, 2008).

12. Thomas v. State, 993 So. 2d 105, 107–08 (Fla. Dist. Ct. App. 2008).

13. *Canatxx Gas*, 2008 U.S. Dist. LEXIS 37803 at *37; *Microsoft*, 2002 U.S. Dist. LEXIS 7683 at *2.

14. DirecTV, Inc. v. Murray, 307 F. Supp. 2d 764, 772–73 (D.S.C. 2004).

15. Fed. R. Evid. 802(d)(2)(A).

16. Fed. R. Evid. 802(d)(2)(E).

17. *See* Bourjaily v. United States, 438 U.S. 171, 175 (1987).

18. *See* United States v. Geaney, 417 F.2d 1116, 1120 (2d Cir. 1969) ("While the practicalities of a conspiracy trial may require that hearsay be admitted 'subject to connection,' the judge must determine, when all the evidence is in, whether . . . the prosecution has proved participation in the conspiracy. . . .").

19. United States v. Tellier, 83 F. 3d 578, 580 (2d Cir. 1996).

20. Fed. R. Evid. 801(d)(2)(B).

21. *Safavian*, 435 F. Supp. 2d at 43–44.

22. United States v. Joe, 8 F.3d 1488, 1493 (10th Cir. 1993).

23. Brill v. Lante Corp., 119 F.3d 1266, 1271 (7th Cir. 1997).

24. *Safavian*, 435 F. Supp. 2d at 36.

25. Demarco v. Lehman Brothers Inc., 309 F.Supp.2d 631 (S.D.N.Y. 2004).

26. Jamsports & Entm't, LLC v. Paradama Prods., 336 F. Supp. 2d 824 (N.D. Ill. 2004).

27. SEC v. Mozilo, 2009 U.S. Dist. LEXIS 104689 (C.D. Cal. Nov. 3, 2009).

28. Pursuit Partners, LLC v. UBS AG, 2009 Conn. Super. LEXIS 2313 (Super. Ct. Conn. Sept. 8, 2009).