

## Project: Corporate Counsel – Legal Service Providers

# Learning From Wall Street's E-Mail Nightmare: Discovery And Admissibility Of E-Mail

By Patrick J. Burke

Wall Street firms have learned a painful lesson about e-mail over the past months, and corporate investigations and discovery likely will never be the same. Their e-mail nightmare is a wake-up call for in-house litigators in all industries. There was a time when lawyers might reasonably have advised their clients to purposely keep e-mails inaccessible to discourage intrusive discovery. Recent events demonstrate that the days of avoidance are gone forever.

Because nMatrix offers the leading proprietary software for converting e-mail into databases for archiving and litigation support, we have become familiar with many of the pertinent legal issues. This article provides a short overview of the federal requirements for discovery and admissibility of e-mail, with recommendations as to the technology lawyers should demand to help them confront the challenge of e-mail as evidence.

### Discovery Of E-Mail In Federal Litigation

Discovery of e-mail in federal civil litigation is becoming broader and more common. Though the Federal Rules of Civil Procedure do not refer to e-mail explicitly, courts agree that e-mail is plainly within the scope of materials that must be produced in connection with voluntary early disclosure under Rule 26(a)(1)(B) and discovery under Rule 34.<sup>1</sup> Beyond that broad conclusion, however, there is little consensus on how such disclosure and discovery of e-mail should be conducted.<sup>2</sup>

*Volume of e-mail to be produced.* Responsive e-mails often dramatically exceed the number of responsive traditional paper documents, particularly given the large numbers of "backup" copies of e-mail kept by companies (hence the importance of de-duplication capability in e-mail archiving technology). Given the massive volumes, courts often apply the "proportionality" limitations of Rule 26, which authorizes limiting discovery where "the burden or expense of the proposed discovery outweighs its likely benefit..."<sup>3</sup>

*Mode of delivery.* Paper has been the standard format for years and is often preferred by respondents because it is more difficult and expensive for opposing counsel to manage, and because printed e-mails do not include the metadata that can contain valuable information.<sup>4</sup> Gradually, litigators are recognizing the irrationality of converting e-mail into paper and back. Rules



Patrick J. Burke

26 and 34 are silent on e-mail and how it should be produced.<sup>5</sup> Courts have yet to find consensus on the appropriate format for delivery of e-mail.<sup>6</sup> Nonetheless, courts have increasingly ordered — and parties have increasingly agreed to — the production of e-mails in electronic format. Courts have variously ordered production of e-mails in electronic format,<sup>7</sup> or arrived at some compromise.<sup>8</sup>

*How to organize e-mail produced in paper format pursuant to Rule 34.* Rule 34 states that a party shall produce documents for inspection "as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the request."<sup>9</sup> How does one meet either of these two requirements with respect to e-mail, where with the click of a key individuals can reshuffle their e-mail folders many times a day? The law is not settled.

### Duty To Locate And Preserve E-Mail, And Sanctions For Failure To Produce Discoverable E-Mail

At the onset of litigation, it becomes the duty of the firm's attorneys to identify and preserve e-mail that may be required to be disclosed under Rule 26(b)(1) and Rule 34, i.e., e-mails relating to the claim or defense of a party to the suit. In the initial voluntary disclosure phase, Rule 26(a)(1) is read in tandem with Rule 26(g)(1), which imposes a duty of reasonable inquiry in connection with mandatory disclosures, with a party deemed put on notice of e-mails' possible relevance once litigation has begun.<sup>10</sup> Once litigation is imminent or has commenced, severe sanctions may be imposed for the destruction of relevant e-mails.<sup>11</sup> These sanctions are wide-ranging under Rule 37 (or under a court's inherent authority), but must be proportionate to the circumstances surrounding the failure.<sup>12</sup> However, a company's culpability in failing to adjust or stop its record-disposition practices due to pending litigation may be mitigated if the requesting party fails to notify the responding party to do so in a timely manner.<sup>13</sup>

### Admissibility Of E-Mail In Federal Courts

E-mail generally faces two objections to admission as evidence at trial: hearsay and foundation (authentication).

Clearly e-mail is an out-of-court statement and, if it is offered for the truth of what it asserts, it is likely to face an objection on the grounds that it constitutes hearsay. Hearsay is not applicable, however, where e-mails are not being offered for the truth of what they assert, but merely to impeach the credibility of witnesses.

### Admission Of E-Mails As Exceptions To The Hearsay Rule

The most viable and frequently used hearsay exception with respect to e-mail is to characterize it as a business record under Federal Rule of Evidence 803(6) ("FRE 803(6)"), the "business records exception."<sup>14</sup> Not all e-mails, or all business records, qualify under the business records exception, which consists of five elements: (1) the record must be kept in the course of a regularly conducted business activity; (2) the particular record at issue must be one that is regularly kept; (3) the record must be made by, or from, information transmitted by a person with knowledge of the source; (4) the record must be made contemporaneously; and (5) the record must be accompanied by foundation testimony.<sup>15</sup>

### Foundation: Authentication Of E-Mail

All documents admitted as evidence must first be authenticated.<sup>16</sup> Computerized business records are admissible under essentially the same conditions as non-computerized records; no additional authenticating evidence is required just because the records are computerized.<sup>17</sup> In the case of documents admitted pursuant to the business records exception to the hearsay rule, the Federal Rules of Evidence require the testimony of the "custodian" of the information or some "other qualified witness" that the e-mail was "kept in the course of a regularly conducted business activity, and if it was a regular activity to make" such documents.<sup>18</sup> The foundation witness need not have been employed by the organization at the time the e-mail was written and sent, so long as he or she can testify to the recordkeeping practices at that time.<sup>19</sup> In fact, it is well worth arranging in advance that a knowledgeable representative of your e-mail archive software provider be prepared to act as a foundation witness with respect to the admission of firm e-mail as business records.<sup>20</sup>

When seeking admission of e-mail pursuant to an exception to the hearsay rule other than the business records exception, e-mail must comply with the general requirement of FRE 901 of authentication prior to admission. "E-mail messages can generally be authenticated by the same types of circumstantial evidence that are used to authenticate any other correspondence."<sup>21</sup> Paper copies of e-mails produced by a party during discovery may be authenticated by the very act of their production.<sup>22</sup>

### What Lawyers Should Demand From E-Mail Archive Technology

In-house counsel should view smart

e-mail archiving technology as an opportunity for their law department to save their business clients significant costs whenever investigations or litigation arise. These savings will come through swifter and less costly fact investigations and more cost-effective production of materials to regulators and adversaries. Here is the checklist of features in-house counsel should seek in an e-mail archive system:

- Same-day capture of all employees' e-mail.
- E-mails go directly into a fully searchable, image-enabled database.
- Ability to apply privilege/witness/issue coding to e-mail in the database.
- Ability automatically to monitor, identify, and route potential problem e-mails for immediate compliance or investigatory examination.
- Ability to bates-stamp, affix labels, and organize e-mails for production to regulators, adversaries, and outside counsel.
- De-duplication of e-mails collected.
- Strategy for authentication at trial.

The right e-mail archive technology offers a smarter and more cost-effective system to monitor compliance, satisfy investigators, comply with discovery requests, and secure admissibility of critical evidence in litigation. A choice of technology that ignores the attorneys' checklist of desired features puts all of that at risk, and could well cause the firm tens if not hundreds of millions of dollars in avoidable costs.

<sup>1</sup> Federal Rules of Civil Procedure 26(a)(1)(B) and 34(a) call for the disclosure and discovery of "data compilations." See also 7-37A Moore's Federal Practice §37A.10[2] ("Rule 34 Applies to Production of Computer-Based Information").

<sup>2</sup> Hon. Shira A. Scheindlin and Jeffrey Rabkin, "Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?" 41 B.C. L. Rev. 327, 350-361 (March 2000).

<sup>3</sup> Fed. R. Civ. P. 26(b)(2); see, e.g., 41 B.C. L. Rev. at 349.

<sup>4</sup> An explanation of the type of information not conveyed by a printout of an e-mail is provided in *Armstrong v. Executive Office of the President*, 1 F.3d 1274, 1280 (D.C. Cir. 1993).

<sup>5</sup> Fed. R. Civ. P. 26(a)(1)(B), 34(a).

<sup>6</sup> 41 B.C. L. Rev. at 346-51. The authors, one a respected U.S. District Court Judge in the Southern District of New York, suggest relatively simple amendments to Rules 26 and 34 to solve the inherent definitional and logistical difficulties in applying the rules to electronic discovery. *Id.*, at 371-79.

<sup>7</sup> See, e.g., *Sattar v. Motorola, Inc.*, 138 F.3d 1164, 1171 (7th Cir. 1998).

<sup>8</sup> See, e.g., *Playboy Enters. v. Welles*, 60 F. Supp. 2d 1050, 1054 (S.D. Cal. 1999), *aff'd* in pertinent part, *rev'd* in part, remanded by 279 F.3d 796 (9th Cir. Cal. 2002); *Linnen v. A.H. Robbins Co.*, 1999 Mass. Super. LEXIS 240, at \*16-19 (Mass. Super. Ct. June 15, 1999); *In re Brand Name Prescription Drugs Antitrust Litig.*, 1995 U.S. Dist. LEXIS 8281, at \*7-8 (N.D. Ill. June 13, 1995).

<sup>9</sup> Fed. R. Civ. P. 34(b).

<sup>10</sup> Fed. R. Civ. P. 26(a)(1), 26(g)(1). 7-37A Moore's Federal Practice—Civil § 37A.33[3] & n.7.

<sup>11</sup> 7-37A Moore's Federal Practice §37A.12[5][d][iii].

<sup>12</sup> See, e.g., *Anderson v. Beatrice Foods Co.*, 900 F.2d 388, 395 (1st Cir. 1990), *cert. denied*, 498 U.S. 891 (1990).

<sup>13</sup> See, e.g., *New York State NOW v. Cuomo*, 1998 U.S. Dist. LEXIS 10520, at \*7-9 (S.D.N.Y. July 13, 1998).

<sup>14</sup> Fed. R. Evid. 803(6).

<sup>15</sup> *Id.*

<sup>16</sup> Fed. R. Evid. 901.

<sup>17</sup> Weinstein's Federal Evidence §901.08[1] (2002).

<sup>18</sup> Fed. R. Evid. 803(6).

<sup>19</sup> See *United States v. Evans*, 572 F.2d 455, 490 (5th Cir.), *cert. denied*, 439 U.S. 870 (1978); *United States v. Rose*, 562 F.2d 409, 410 (7th Cir. 1977).

<sup>20</sup> Sometimes a vendor provides expert testimony that demonstrates conclusively that an e-mail is inauthentic. See *Suni Munshani v. Signal Lake Venture Fund II, LP*, 00-5529 BLS, 2001 Mass. Super. LEXIS 496 (October 9, 2001) (where report by e-mail forensics expert determined that key e-mail upon which plaintiff's case relied "is clearly not authentic," resulting in dismissal of action and sanctions against plaintiff for fraud on the court).

<sup>21</sup> Weinstein's Federal Evidence §901.08[3] (2002); see, e.g., *United States v. Briscoe*, 896 F.2d 1476 (7th Cir. 1990).

<sup>22</sup> Weinstein's Federal Evidence §901.08[3] (2002) (citing Fed. R. Evid. 902(7)).

Patrick J. Burke is Technology Counsel at nMatrix, Inc., a New York City-based software development company serving major law firms and law departments and the maker of eDataMatrix™ software for conversion and archiving of e-mail ([www.nmatrix.com](http://www.nmatrix.com)). This article is adapted from a much longer article published in *The Journal of Investment Compliance, Summer 2002* (available on the nMatrix website at [www.nmatrix.com/wall\\_street\\_email](http://www.nmatrix.com/wall_street_email)).