New York Law Journal

A NEW YORK LAW JOURNAL SPECIAL SECTION

INVESTIGATIONS & COMPUTER FORENSICS

Tuesday, May 30, 2006

ALM

Government Investigators Focus In on E-Mail

With requests for not only full, but fast, subpoena compliance, corporate entities face significant challenges to which the key is preparation.

BY SCOTT A. RESNIK

E-MAIL HAS TRANSFORMED the way the world communicates and does business. It also has become a highly sought-after form of evidence in white-collar criminal and regulatory investigations.

As an increasing percentage of business communication is entrusted to e-mail, conversations that once passed and vanished over telephone lines or on readily discarded fax pages, now lay preserved for years—often unbeknownst to their creator—electronically chiseled into a server, hard drive or back-up tape. A stored e-mail has the potential to provide an investigator with a trove of information, from the text of a past conversation, to the substance of attached files, to a catalogue of recipients and copied parties. For the government investigator, stored e-mails have the ability to narrate past crimes or regulatory violations and identify co-conspirators through frozen-in-time communications with a clarity and ease that was unimaginable a short time ago.

It took law enforcement and regulatory agencies a while to appreciate the bounty offered by this electronic document trail and harness the human and technological resources needed to tap into this information source. But with increased staffing and the tools of computer forensics, the days when a government investigator could be dissuaded by skilled counsel from putting a company through the rigors of collecting e-mails in response to a subpoena are gone for good. In fact the pendulum has swung in the opposite direction.

The opening salvo of a white-collar criminal or regulatory investigation will likely be a corporate subpoena featuring a request for relevant e-mails. A company's ability to gather, to the government's satisfaction, relevant e-mail will impact dramatically on the government's view of whether the company is cooperating with, or hindering, the investigation. The consequences of such a determination can, obviously, be dire.

While there is nothing new in the observation that shoddy subpoena compliance is a sure way to run afoul of government investigators, e-mail compliance poses additional pitfalls for the unprepared. With heightened investigatory focus on electronic evidence, prosecutors and regulators are insisting on e-mail compliance on expedited time schedules from subpoenaed companies. Compliance must not only be full, but fast.

The challenge this poses to corporate entities with thousands of individuals and a panoply of e-mail accounts, hard drives, servers, back-up tapes, PDAs and laptops, is significant. A subpoenaed company acting in good faith to comply and cooperate with the government can still suffer dramatic consequences if it cannot adequately harness its e-mail systems to make complete and timely productions.

Indeed, in-house counsel who wait until a subpoena arrives to begin familiarizing themselves with the strengths and weaknesses of their e-mail systems, place themselves and their company at a distinct disadvantage. And as the emerging legal landscape warns, the consequences can be significant.

ART BY ISTOCK

The Compliance Environment

The challenge of electronic evidence compliance begins with the heightened expectations of investigating agencies. Most regulators and prosecutors are far removed from the technological challenges facing modern companies.

Government investigators often take a broad-brush approach to demands for electronic discovery. The prevailing mind-set remains that electronic communications are easy for a corporation to preserve and produce. Further, law enforcement's concern that electronic information remains susceptible to destruction or tampering reinforces their instinct to insist on prompt production.

Corporate counsel faced with grand jury or regulatory subpoenas for electronic communications in this environment must be prepared to act quickly and comprehensively. A

Scott A. Resnik *is a litigation partner in the New York office of Katten Muchin Rosenman, and a member of the firm's white collar criminal and civil litigation group.*

company's opportunity to cooperate with the authorities and negotiate a favorable resolution of the investigation will be heavily influenced by its ability to comply fully and expeditiously with the government's subpoena. This is especially so in the securities industry, where the Securities and Exchange Commission requires broker-dealers to preserve business-related e-mails for three years, and to keep two years' worth of stored e-mails available for "prompt" production to the Commission if requested.[1]

Anticipate and Prepare

In such an atmosphere of heightened compliance expectations, corporate counsel cannot, as already noted, wait for the arrival of a regulatory subpoena to begin familiarizing themselves with the capabilities of their firm's electronic document retention and retrieval capabilities.

Counsel best positioned to handle the crisis of an investigation are those who have already established a working relationship with their company's information technology department and are knowledgeable of data storage policies and procedures. Armed with this information, counsel can effectively interface with the regulator or prosecutor and negotiate meaningful limitations to the scope of the subpoena and adjustments to the time frame of compliance. It will also enable counsel to make appropriate representations to regulators concerning the company's compliance with applicable industry regulations on the storage of electronic communications.

Conversely, if counsel is unfamiliar with e-mail retention policies and recovery capabilities, initial negotiations with the investigators can be counter-productive. Setting deadlines that cannot be met, or unintentionally misrepresenting what can be produced, will quickly sour relations with the investigating agency and often doom any attempts at cooperation.

A company's obligation to preserve potentially relevant e-mails likewise does not necessarily require the arrival of a subpoena to be triggered. While the receipt of a criminal or regulatory subpoena clearly places a duty upon a company to preserve responsive documents and halt any regular destruction procedures, companies are well advised to begin preservation efforts when an investigation becomes reasonably foreseeable.

In *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003), the district court, addressing the preservation of electronic evidence in the context of an employment discrimination case, held that "the obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant in future litigation." Accordingly, "once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents." Id. at 218.

Zubulake's forward-looking preservation rule would likely apply with equal force in the context of an anticipated government investigation. Prudent corporate counsel, post-*Zubulake*, therefore, should begin preserving electronic evidence once a criminal or regulatory investigation becomes reasonably foreseeable.

A failure to preserve electronic communications in the face of a foreseeable investigation invites great risk. An intentional failure to preserve such evidence can lead to criminal prosecution for obstruction of justice.[2] Even an unintentional failure to halt the destruction of relevant electronic evidence can result in sanctions.

Illustrative is *MOSAID Tech. Inc. v. Samsung Elecs. Co.*, 348 F. Supp. 2d 332, 337-38 (D.N.J. 2004), where the court concluded that even in the absence of bad faith, a company's failure to put a litigation hold on e-mail, which resulted in the prejudicial destruction of relevant technical e-mail, warranted an adverse inference instruction and monetary sanctions.[3]

With increased staffing and the tools of computer forensics, the days when a government investigator could be dissuaded by skilled counsel from putting a company through the rigors of collecting e-mails in response to a subpoena are gone for good.

This refusal to require bad faith as a prerequisite to imposing sanctions provides convincing evidence that courts are joining with investigators in growing increasingly intolerant of companies that do not adequately preserve and produce electronic communications. In appropriate cases, it is not uncommon for courts to enter orders requiring the preservation of potentially relevant electronic evidence. When parties fail to abide by such orders, the consequences are predictably dire.[4]

Can You Assure Full Compliance?

Similarly, to promote accountability in electronic document productions, the SEC often seeks an assurance of full compliance from the respondent company. In addition, it is standard for the SEC to require a company, as part of any settlement agreement, to certify in writing, under penalty of perjury, that it has produced all required documents.[5]

To be in a position to satisfy either of these obligations, counsel must ensure that their client's retention and collection efforts are thorough and well-documented. Pre-investigation efforts by counsel to ensure that the right personnel are involved with compliance, and that procedures are in place to both avoid the destruction of relevant e-mails and to ensure the full recovery of stored messages, will pay dividends when the time for assurances or certification comes.

The SEC has imposed some jaw-dropping fines in resolving investigations of corporate wrongdoing where corporate assurances of complete electronic discovery compliance were later revealed to have been inaccurate.

In *SEC v. Deutsche Bank Securities Inc.*, Litigation Release No. 18854 (Aug. 26, 2004), the SEC imposed a $7.5 million fine on Deutsche Bank (DB) (in addition to the $50 million fine to resolve the underlying investigation into research analyst conflicts of interest) for failing to "timely produce all e-mail during the investigation." DB's trouble began after it had made assurances to the SEC that its production of requested e-mail was complete.

Over the course of the next year, however, DB discovered and produced an additional 227,000 e-mails, more than tripling its original "complete" production. Id. The SEC blamed this compliance failure with delaying the completion of the investigation for over a year and fined DB accordingly. Id.

Similarly, in *In the Matter of JPMorgan Securities, Inc.*, Admin. Proc. File No. 3-11828 (Feb. 15, 2005), during an investigation of stock analyst misconduct, JPMorgan made repeated representations that all relevant e-mail requested by the Commission had been produced. Subsequently, in response to further requests by the SEC, JPMorgan revealed that it had been unable to locate and restore certain backup tapes containing responsive e-mail. For this failure, which was disclosed months into the investigation, JPMorgan agreed to settle with the SEC, NYSE and NASD for $2.1 million in fines. Id.[6]

The consequences of making a knowingly false certification of compliance to a court were starkly spelled out in *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, Case No. 502003-CA-005045, 2005 WL 679071 at *1-*5 (Fla. Cir. Ct. March 1, 2005). The Florida state court gave the jury a detailed adverse inference charge after Morgan Stanley was discovered to have made a knowingly false certification that it had complied with a court order requiring the complete production of e-mail evidence.

Morgan Stanley had submitted the certification knowing that it had failed to search or produce over 2,000 backup tapes and had continued to delete e-mails on a 12-month schedule in violation of the SEC rule that e-mails be maintained for three years. The jury verdict against Morgan Stanley awarded over $604 million in compensatory damages and $850 million in punitive damages.

To make matters worse for Morgan Stanley, the revelation of its e-mail retention policies attracted the attention of the SEC. In February 2006, MS agreed to settle with the SEC for a record $15 million in fines as a result of its failure to properly maintain its e-mail records in accordance with SEC regulations.[7]

Timing Is Everything

Timing is the other critical factor in compliance with requests for electronic discovery.

Even for the respondent company that can efficiently retrieve requested e-mails, time remains a valuable commodity. This is because one of coun-

sel's primary responsibilities in subpoena compliance is to preserve privilege. And to review a sizeable collection of responsive e-mails for privilege is going to take a significant amount of time.

This reality creates an inherent tension with the government investigator whose instinct is to demand expeditious production. It further emphasizes why the data collection process must be swift. Time lost in retrieving responsive documents will further erode counsel's time to review the data collection to ensure that privileged documents are not disclosed to the government. Even inadvertent disclosure of privileged documents may result in a waiver of the attorney-client privilege.[8]

One strategy for reducing delay frequently advocated by the government is for the respondent company to produce the requested e-mail without attorney review, but with an agreement that the government will not assert waiver if the production contains attorney-client communications or attorney work product. This strategy is fraught with danger for the respondent company. In addition to divulging the substance of critical communications, such an approach can have unintended consequences on the attorney-client privilege in subsequent litigation.[9]

In the context of private-party civil litigation, sanctions are rarely imposed for mere delay in producing electronic discovery.[10] In the realm of regulatory investigations, however, there is evidence of a countervailing trend.

In a recent action, the SEC imposed a $2.5 million fine on broker Merrill Lynch for "failure to furnish promptly to representatives of the Commission…electronic mail communications" as required under §17(a) of the Exchange Act and enabling regulations. *In the Matter of Merrill Lynch, Pierce, Fenner & Smith, Inc*., Admin. Proc. 3-12236 (March 13, 2006). The case is noteworthy because the SEC release does not identify any substantive wrongdoing on the part of Merrill Lynch (ML) nor any failure to produce critical e-mails. The sanction is based solely on the firm's slow compliance response and inadvertent short-comings in its e-mail capture system. Because of this, it is worth a closer look.

From October 2003 through February 2005, the SEC requested that ML produce e-mails in connection with a series of separate investigations. On Oct. 17, 2003, the SEC requested the production of e-mails from six ML employees. Id. at 2. It took ML seven months to produce the requested e-mails. Id.

Also in October 2003, the Commission issued a request in another investigation for the e-mails of five ML employees. ML took two months to begin making its production and completed delivery of the requested e-mails five and one-half months from receipt of the Commission's request. Id. at 3.

In two other investigations in August and September 2004, it took ML over five months to produce requested e-mails. Id. Further aggravating the situation from the SEC's perspective were ML's representations that its e-mail systems were sufficient to retain e-mail and produce it to regulators upon demand. Id.

It was subsequently discovered that ML's e-mail systems were not capturing (a) e-mails that were not in a user's mailbox at the time of the next scheduled tape back-up; (b) e-mail that had been moved from a user's mailbox to a personal folder or shared drive outside the e-mail system or moved to another medium such as a floppy disk, a hard drive, or a USB (universal serial bus) device; (c) e-mail that had been "hard-deleted" prior to the next scheduled tape back-up; and (d) "bcc" recipients on certain e-mail messages. Id.

Based on these technological shortcomings and its slow compliance response, the Commission took the position that ML was in violation of its document retention obligations under the Exchange Act. The settlement not only required ML to pay a fine of $2.5 million, but also to hire at its own expense an independent consultant to review ML's e-mail retention policies and procedures. Id. at 5-7.

Time lost in retrieving responsive documents will further erode counsel's time to review the data collection to ensure that privileged documents are not disclosed to the government.

The *Merrill Lynch* decision demonstrates the potential of electronic discovery to become the "tail that wags the dog" in regulatory investigations.[11] Even in the absence of substantive wrongdoing, a corporation remains vulnerable to dramatic fines if it fails to meet the regulator's timetable for compliance.

The decision makes clear that from the Commission's perspective, five months to produce e-mail was too long. Observers, though, are left to speculate on what time frame, given these circumstances, would have been acceptable. Nonetheless, the decision puts companies on notice that those who fail to act expeditiously in complying with requests for electronic communications, do so at their own risk.

Conclusion

The challenges of responding to an investigator's request for corporate e-mail are many but they are not insurmountable. The key is preparation.

Companies must establish and continually review their electronic document retention and production policies to ensure that once an investigation becomes foreseeable, responsive documents are preserved and can be timely collected. Counsel should be knowledgeable of their clients' technological capabilities and establish working relationships with their IT staff.

If faced with the same requests for e-mail as confronted in *Merrill Lynch*, would your company be able to produce the information in under five months? Can your e-mail system capture "bcc" recipients? If you do not know the answer to these questions, the time to figure it out is now. Not when an SEC subpoena arrives.

1. Rule 17a-4(b)(4), promulgated pursuant to §17(a) of the Exchange Act, requires broker-dealers to "preserve for a period of not less than three years, the first two years in an easily accessible place…[o]riginals of all communications received and copies of all communications sent…(including inter-office memoranda and communications) relating to its business as such…." 17 C.F.R. 240.17a-4(b)(4). E-mail communication falls within this rule. See *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 308, 314 (S.D.N.Y. 2003). Further, Rule 17a-4(j) requires broker-dealers, upon request of the SEC, to "furnish promptly" any records required to be preserved by §17(a) of the Exchange Act. 17 C.F.R. 240.17a-4(j).

2. See, e.g., 18 U.S.C. §1512(c)(1) ("Whoever corruptly alters, destroys, mutilates, or conceals a record, document, or other object, or attempts to do so, with the intent to impair the object's integrity or availability for use in an official proceeding [commits a federal crime]"); 18 U.S.C. §1519 ("Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record…with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States…[commits a federal crime]").

3. See also *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99 (2d Cir. 2002) (holding that negligent destruction of potentially relevant electronic data can be an appropriate basis for discovery sanctions); *Telecom Int'l Am., Ltd. v. AT&T Corp.*, 189 F.R.D. 76, 82 (S.D.N.Y. 1999) (holding that defendant's destruction of documents, even though not committed in bad faith, demonstrated an "indifference to…discovery obligations" that required the imposition of appropriate sanctions).

4. See *United States v. Philip Morris USA Inc*., 327 F. Supp. 2d 21, 24-6 (D.D.C. 2004) (imposing $2.75 million sanction, ordering party to pay costs related to spoliation and prohibiting party from calling certain witnesses where party did not put in place a litigation hold and permitted routine destruction of relevant e-mail for two years after the court entered a document-retention order).

5. See John Savarese and Carol Miller, "Effective Strategies for Defending Investigations, Sept. 14, 2005," in "Coping With Broker/Dealer Regulation & Enforcement 2005" at 266 (PLI 2005).

6. See also *In Matter of UBS Securities LLC*, Admin. Proc. File No. 3-11980 (July 13, 2005) (for failure to produce relevant e-mail for each individual identified in investigation, UBS agreed to pay $70,000 in fines to SEC, NYSE and NASD).

7. See Bruce Kelly, "E-mail Troubles Continue to Haunt Broker-Dealers, Morgan Stanley to Pay $15 Million Fine," Investment News, Feb. 20, 2006, at 33.

8. See *Genetech, Inc. v. U.S. Int'l Trade Comm'n*, 122 F.3d 1409, 1417 (Fed. Cir. 1997) (holding party's waiver of attorney-client privilege with regards to documents it inadvertently disclosed during patent infringement litigation was general waiver that could be asserted in administrative proceeding before the International Trade Commission); *F.D.I.C. v. Singh*, 140 F.R.D. 252, 253 (D. Me. 1992) (holding inadvertent production of memorandum containing privileged communications constituted waiver of attorney-client privilege).

9. See *In re Columbia/HCA Healthcare Corp. Billing Practices Litig.*, 293 F.3d 289, 302 (6th Cir. 2002) (holding party could not selectively waive attorney-client privilege by providing otherwise privileged documents to government agencies during an investigation but continue to assert privilege as to private litigants).

10. See Shira A. Scheindlin and Kanchana Wangkeo, "Electronic Discovery Sanctions in the Twenty-First Century," 11 Michigan Telecomm. and Tech. L. Rev. 71, 76 (2004) ("The sanctioned behavior most often involved the non-production, i.e., destruction of electronic documents (84%), rather than a delay in production (16%). When parties were sanctioned for delay, the late production was sometimes coupled with some form of deception or misrepresentation to the court, such as the fabrication of evidence or falsely claiming that documents did not exist (43%)").

11. See Terry Weiss, "Summary of Selected Programs From SIA Compliance & Legal Division's 2006 Annual Seminar," Mondaq Bus. Briefing, April 3, 2006 ("The failure to retain and produce electronic data when required to do so has become an independent source of potential liability regardless of any underlying wrongdoing, panel members cautioned…'The tail is now wagging the dog,' the panel warned").